Máster Universitario en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas

Trabajo Fin de Máster

La Ciberseguridad en Educación Secundaria: Análisis contextual y propuesta de recurso digital

GL: A Ciberseguridade en Educación Secundaria: Análise contextual e proposta de recurso dixital

EN: Cybersecurity in Secondary Education: Context analysis and digital resource proposal

Autor: *Alberto Pampín Pérez*

Dirección: *Silvia López Gómez*

Curso 2022 - 2023

Trabajo de Fin de Máster presentado en la
Facultad de Ciencias de la Educación de la Universidad de Santiago de Compostela
para la obtención del Máster Universitario en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas

Hoja de autorización

Trabajo Fin de Máster presentado en la Facultad de Ciencias de la Educación de la Universidad de Santiago de Compostela por Alberto Pampín Pérez, como requisito para obtener el título de Máster Universitario en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas que cuenta con la autorización y dirección de Silvia López Gómez, para su presentación y defensa.

Dirección,

Silvia López Gómez

Autor,

Alberto Pampín Pérez

Firmado por
PAMPIN PEREZ
ALBERTO -
46092244Z el día
19/06/2023 con

Resumen

ES: Este Trabajo Fin de Máster (TFM) tiene como propósito fundamental analizar el impacto de los riesgos asociados a las TIC e Internet sobre la sociedad, prestando especial atención a la adolescencia. Asimismo, tras los resultados obtenidos en el análisis realizado, se ha desarrollado y evaluado CYBERTOWN 2D[1] un recurso digital orientado al alumnado de Educación Secundaria Obligatoria (ESO) que ayuda a mejorar los conocimientos en Ciberseguridad. Para el cumplimiento de ambas finalidades, en este trabajo se identifican las principales investigaciones en este ámbito, así como las campañas, servicios y recursos ofrecidos por la Administración Pública. Además, se analiza el currículum de la ESO en Galicia en materia de Ciberseguridad y se exponen los resultados obtenidos tras aplicar un cuestionario *on-line* sobre Ciberseguridad, el cual contó con un total de 1120 participantes, entre los que se incluye alumnado de ESO, profesorado y familias. De este trabajo se puede concluir que la ciudadanía carece de los conocimientos suficientes en Ciberseguridad, por lo que resulta indispensable seguir trabajando en este ámbito y desarrollar recursos efectivos como CYBERTOWN 2D.

Palabras clave: *Ciberseguridad, Internet, Educación Secundaria y Material Didáctico Digital*

GL: Este Traballo de Fin de Máster (TFM) ten como propósito fundamental analizar o impacto dos riscos asociados ás TIC e Internet sobre a sociedade, prestando especial atención á adolescencia. Así mesmo, tras os resultados obtidos na análise realizada, desenvolveuse e avaliouse CYBERTOWN 2D[1], un recurso dixital orientado ao alumnado de Educación Secundaria Obrigatoria (ESO) que axuda a mellorar os coñecementos en Ciberseguridade. Para o cumprimento de ambas finalidades, neste traballo identifícanse as principais investigacións neste ámbito, así como as campañas, servizos e recursos ofrecidos pola Administración Pública. Ademais, analízase o currículo da ESO en Galicia en materia de Ciberseguridade e expóñense os resultados obtidos tras aplicar un cuestionario *on-line* sobre Ciberseguridade, o cal contou cun total de 1120 participantes, entre os que se inclúe alumnado de ESO, profesorado e familias. Deste traballo pódese concluír que a cidadanía carece dos coñecementos abondos en Ciberseguridade, polo que resulta indispensable seguir traballando neste ámbito e desenvolver recursos efectivos como CYBERTOWN 2D.

Palabras chave: *Ciberseguridade, Internet, Educación Secundaria e Material Didáctico Dixital*

EN: This Master's Thesis (TFM) aims to analyze the impact of risks associated with ICT and the Internet on society, with a special focus on adolescence. Furthermore, based on the results obtained from the conducted analysis, CYBERTOWN 2D[1], a digital resource targeting Secondary Education students, has been developed and evaluated to enhance knowledge in Cybersecurity. To fulfill these objectives, this work identifies the main research in this field, as well as the campaigns, services, and resources provided by the Public Administration. Additionally, the curriculum in Galicia for Secondary Education regarding Cybersecurity is analyzed, and the results obtained from an online Cybersecurity questionnaire are presented. The questionnaire had a total of 1120 participants, including students, teachers, and families from Secondary Education. From this study, it can be concluded that the general population lacks sufficient knowledge in Cybersecurity, highlighting the need to continue working in this area and developing effective resources such as CYBERTOWN 2D.

Keywords: *Cybersecurity, Internet, Secondary Education and Digital Teaching Material*

[1] CYBERTOWN 2D: https://view.genial.ly/6361673e32a5d700111c03ae/interactive-content-cybertown2d

Índice general

Índice de figuras

Introducción

En la era digital, la tecnología e Internet se han convertido en elementos esenciales, transformando la forma en que interactuamos, nos comunicamos y accedemos a la información. Sin embargo, junto con sus numerosos beneficios, también surgen infinidad de desafíos y uno de los más apremiantes es la Ciberseguridad. El uso masivo de las Tecnologías de la Información y la Comunicación (TIC) ha motivado a individuos maliciosos a emplear estos nuevos recursos para lucrarse del desconocimiento de los demás. Ataques como el *phishing* no hacen más que aumentar y otros como el *ransomware* alcanzan máximos históricos (APWG, 2022). Por otra parte, la ciudadanía carece de los conocimientos necesarios para identificar y protegerse de estos riesgos. Según un estudio realizado por el Instituto Nacional de Ciberseguridad de España (INCIBE, 2022b), un 25 % de los encuestados ignoran el significado del cifrado de datos y casi un 40 % reconoce no saber si su dispositivo está actualizado o no. Aunque todos los riesgos se suelen atribuir a los tan temidos *hackers*, lo cierto es que gran cantidad de ellos están asociados a las prácticas de riesgo de los propios usuarios, como por ejemplo el *sexting*, el *revenge porn* y la *sextortion* - los cuales suelen derivar del primero -, el *grooming* y el *cyberbullying*. Estas prácticas son especialmente relevantes en la adolescencia, donde a la gran cantidad de cambios propios de esta época (Steinberg, 2008), se le suma el desconocimiento de los riesgos y los problema de adicción al teléfono móvil y a las redes sociales (Fundación Barrié, 2022).

La sociedad digital actual se encuentra en un momento crítico en lo que respecta a la Ciberseguridad. La Administración Pública es consciente de esta situación y así lo demuestra en la agenda España Digital 2026[2], donde una de sus dimensiones clave consiste en reforzar las competencias digitales de la ciudadanía y garantizar los derechos en el nuevo mundo digital. Para ello, desde la Administración se trata de paliar esta situación mediante campañas de concienciación como #ciberprotégete[3] del INCIBE o Más que un móvil[4] de la Agencia Española de Protección de Datos (AEPD). Desde la Oficina de Seguridad del Internauta (OSI) e Internet Segura For Kids (IS4K), ambas dependientes del INCIBE, se pone a disposición de la ciudadanía multitud de guías, talleres y recursos para potenciar los conocimientos en Ciberseguridad.

[2] Enlace a España Digital 2026: https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx
[3] Enlace a la campaña #ciberprotégete: https://www.incibe.es/ciberprotegete
[4] Enlace a la campaña Más que un móvil: https://www.aepd.es/es/mas-que-un-movil

Entre dichos recursos existen juegos de mesa, recursos interactivos y juegos digitales, los cuales están especialmente enfocados a los más jóvenes. Sin embargo, se considera que estos tienen una serie de aspectos a mejorar en lo que respecta a la significatividad para el jugador y la difusión de las instituciones, servicios y campañas existentes; las cuales desconoce el 50 % de la población (INCIBE, 2022b). Por otra parte, el currículum de la Educación Secundaria Obligatoria (ESO), en un esfuerzo por adaptarse al imparable avance de las TIC, incluye como parte de la Competencia Digital contenidos relativos a la seguridad de los dispositivos, protección de la información personal, prácticas seguras y riesgos...

Con este Trabajo Fin de Máster se pretende analizar el impacto que han tenido y tienen las TIC e Internet sobre la sociedad y la adolescencia, prestando especial atención a los riesgos inherentes de Internet y los esfuerzos de la Administración Pública para proteger y formar a la ciudadanía en este ámbito. Asimismo, se pretende elaborar un recurso digital orientado al alumnado de Educación Secundaria que ayude a mejorar los conocimientos en Ciberseguridad y que dé a conocer las principales campañas, servicios y recursos ofrecidos por las instituciones públicas. Para ello, se establecen los siguientes objetivos principales y específicos:

- Analizar el impacto de los riesgos asociados a las TIC e Internet sobre la sociedad, prestando especial atención a la adolescencia.
  - Identificar los principales estudios e investigaciones que tratan el impacto de los riesgos asociados a las TIC e Internet sobre la ciudadanía y la adolescencia.
  - Evaluar la importancia que se le otorga a la Ciberseguridad en el currículum de la Educación Secundaria Obligatoria en Galicia.
  - Analizar las campañas, servicios y recursos ofrecidos por la Administración Pública.
  - Comprobar el nivel de conocimiento que tiene el alumnado de ESO, profesorado y familias sobre Ciberseguridad: riesgos básicos, instituciones y servicios.
- Elaborar un recurso digital orientado al alumnado de Educación Secundaria que ayude a mejorar los conocimientos en Ciberseguridad.
  - Diseñar e implementar un recurso digital a modo de juego que dé a conocer algunos riesgos básicos, junto con sus consecuencias y medidas de prevención, y difundir las principales campañas, servicios y recursos ofrecidos por la Administración.
  - Evaluar el recurso en un instituto de Educación Secundaria para validar su efectividad.

Marco Teórico

1. Breve contextualización histórica de la tecnología

Durante el último siglo, una serie de acontecimientos ha provocado que la Ciberseguridad sea una de las mayores preocupaciones de la sociedad actual. Comprender esta situación requiere conocer la evolución de Internet desde sus inicios hasta la actualidad, así como de la evolución de las TIC en los centros escolares.

1.1. Evolución histórica de Internet

El evento que dio lugar a lo que hoy conocemos como Internet fue el lanzamiento de la nave Sputnik por parte de la URSS en el año 1957. Como repuesta, el Gobierno de los Estados Unidos formó la Advanced Research Projects Agency (ARPA) dentro del Departamento de Defensa. Gracias a los avances realizados por numerosos científicos, en 1970 se logró la interconexión de cuatro universidades americanas. Esta red se denominó ARPANET y su objetivo era mantener las comunicaciones en caso de guerra. Con el paso de los años, esta red empezó a utilizarse con fines científicos y de colaboración, llegando en 1972 a integrar 50 universidades y centros de investigación dentro de ARPANET. Un año después fue posible la primera conexión entre EE. UU. y Europa. En 1983 el Departamento de Defensa implementó el protocolo de comunicación TCP/IP en la red ARPANET, lo que marcó oficialmente el nacimiento de Internet (Zakon, 2018). En 1991, la propuesta de Tim Berners-Lee - un brillante científico del Conseil Européen pour la Recherche Nucléaire (CERN) - de unir Internet y el Hipertexto, dio lugar a la World Wide Web (WWW), que hoy nos permite acceder a información a través de Internet (Berners-Lee, 2000).

En las últimas décadas, gracias a los grandes avances en el desarrollo de *hardware* y a la reducción de costes propia de las economías de escala, el número de sitios web ha pasado de tan solo 100 en 1993 a, aproximadamente, 1.800 millones (Zakon, 2018). Hoy en día más de 5.450 millones de personas (69 % de la población mundial) disfrutan de acceso a Internet y a las TIC (Internet World Stats, 2022). De acuerdo con International Telecommunication Union (ITU, 2021), en 2020 el 71 % de los jóvenes del mundo - entre 15 y 24 años - utilizaban Internet, en comparación con el 57 % de los otros grupos de edad. Estas cifras varían si nos centramos en los países desarrollados, siendo del 99 % para la juventud y del 87 % en los otros grupos.

1.2. Evolución de las TIC en las escuelas

La primera iniciativa en España de incorporar la tecnología a las aulas tuvo lugar en 1985, cuando el Ministerio de Educación y Ciencia puso en marcha el proyecto Atenea (Arango Vila-Belda, 1984). Ya en el año 1989 había 697 centros adscritos a este proyecto y se llegó a repartir un total de 4.500 equipos informáticos hasta 1992. En Galicia cabe destacar los proyectos Abrente y Estrela, los cuales buscaban la formación del alumnado y profesorado en los nuevos medios informáticos. Durante la década de los 90, debido al abaratamiento de los equipos, los ordenadores se convirtieron en un elemento presente tanto en los hogares como en la escuela, por lo que surgieron más proyectos para la implantación de las TIC (Caballero, 2016).

A partir de los años 2000, cuando la telefonía móvil e Internet comenzaron a llegar a la ciudadanía, el Ministerio de Educación Cultura y Deporte decidió impulsar a nivel nacional el Programa Escuela 2.0 con el objetivo de digitalizar las aulas y dotar al alumnado y profesorado de la formación y recursos pertinentes. En el caso de Galicia se inició el Proxecto Abalar en el curso 2010/2011, donde además de hacer hincapié en la formación, se propuso la creación de un repositorio de contenidos digitales dentro del Espazo Abalar, la plataforma desarrollada por la Consellería de Educación. En 2022 este repositorio cuenta con más de 1.800 recursos digitales disponibles en varios idiomas para Educación Infantil, Primaria, Secundaria, Bachillerato y Ciclos Formativos (Xunta de Galicia, 2022). Según el balance realizado por la Agencia para la Modernización Tecnológica de Galicia (AMTEGA, 2016), entre 2010 y 2014 se equiparon 2.300 aulas y se beneficiaron del programa 50.000 de los 87.000 alumnos que cursaban 5º y 6º de Educación Primaria y 1º y 2º de ESO. También se formó a más de 22.000 docentes y se impartieron actividades destinadas a alumnado, profesorado y familias - Navega con Rumbo - en 668 centros. La ambición del Proxecto Abalar no se queda ahí, ya que desde el curso escolar 2014/2015 se puso en marcha el proyecto Educación Dixital (E-DIXGAL), el cual se trata de la primera implantación del libro de texto digital en los centros gallegos. Siguiendo a Rodríguez Rodríguez y Losada Loureiro (2019), el grado de satisfacción de los docentes con este proyecto es positivo, ya que consideran que la digitalización en el ámbito social y económico no puede dejar de lado al educativo. No obstante, destacan que este nuevo método suele suponer un esfuerzo adicional muchas veces no gratificado y que se debe continuar trabajando en la mejora del proyecto. Actualmente la Xunta de Galicia (2023) continúa apostando por el programa E-DIXGAL, llegando en este curso a más de 60.000 alumnos de 600 centros educativos.

2. Ventajas y malos usos de las TIC e Internet

No cabe duda de que el desarrollo de las TIC e Internet ha cambiado nuestras vidas. Entre los beneficios cabe destacar la revolución de la logística y del comercio en línea, la mejora de la investigación, la salud y la educación, la posibilidad de comunicarnos con nuestros seres queridos de forma ubicua... Sin embargo, el aumento masivo de su uso ha propiciado que muchos utilicen estos nuevos medios con fines maliciosos, por lo que los usuarios deben ser cuidadosos a la hora de utilizar las TIC.

Los riesgos existentes en Internet son numerosos y las cifras de ataques no paran de aumentar. El Anti-Phishing Working Group (APWG, 2022) reportó más de 4.7 millones de ataques *phishing* a nivel mundial durante el 2022, batiendo el récord y colocándose como el peor año que el grupo ha observado. En APWG (2022) también se recoge que los ataques *ransomware* a compañías están en alza, registrando casi 2.500 empresas afectadas en los últimos nueve meses. De acuerdo con el balance realizado por el Instituto Nacional de Ciberseguridad de España (INCIBE, 2022a), en España se han gestionado más de 110 mil incidentes, se han documentado más de 25 mil nuevas vulnerabilidades y se han emitido 555 avisos de seguridad. El reciente estudio llevado acabo por el INCIBE (2022b) buscaba determinar el nivel de conocimiento y preparación de la población española en materia de Ciberseguridad mediante el análisis de sus hábitos y conductas en Internet entre los meses de julio y diciembre de 2021. Para ello, se han comparado datos obtenidos a través de encuestas y del escaneo consentido de dispositivos electrónicos. Los resultados denotan la gravedad de la situación que se vive actualmente: uno de cada cuatro encuestados desconoce qué es el cifrado de datos o de documentos, un 39,6 % no sabe reconocer si su equipo está actualizado o no y casi la mitad de la muestra desconoce la existencia de las campañas sobre Ciberseguridad ofrecidas por la Administración Pública. Esto se traduce en que, durante el último semestre de 2021, el 70,9 % de las personas que se conectaron a Internet han sufrido una situación de fraude. En la mayor parte de los casos fueron invitaciones a visitar webs sospechosas (63,2 %), ofertas de servicios o productos no solicitados (46,5 %) o la solicitud de claves o de información personal (24,3 %). Otra situación que evidencia las carencias de la sociedad en este ámbito fue el experimento de *phishing* llevado a cabo por el Ayuntamiento de Granada a finales de 2022, donde se enviaron 2.200 correos electrónicos a trabajadores y funcionarios públicos, de los cuales 600 cayeron en la estafa y dieron sus claves privadas (Vallejo, 2022).

Los riesgos anteriormente descritos tienen un carácter técnico, de tal forma que aquellos que perpetran los ataquen cuentan con importantes conocimientos técnicos sobre informática y sobre el funcionamiento de Internet. No obstante, no todos los riesgos implican un uso malicioso de la tecnología por parte de algún experto, sino que a menudo son los propios usuarios los que llevan a cabo una serie de prácticas peligrosas. Estas prácticas indebidas cobran especial relevancia en los adolescentes, ya que suele ser el colectivo más vulnerable. Un estudio llevado a cabo por la Fundación Barrié (2022) en Galicia entre más de 10 mil adolescentes mostró que un 95,7 % de ellos tiene su propio teléfono móvil con datos y que un 64,5 % tiene por costumbre llevarlo al centro educativo. Esto facilita el uso de las redes sociales (RRSS), de tal forma que un 78,8 % de ellos está registrado en 3 o más plataformas (YouTube, Instagram, TikTok...) y el tiempo que le dedican es realmente alarmante: un 10,5 % utiliza las RRSS más de 5 horas diarias durante la semana, llegando a ser el 23,7 % los fines de semana. Estos factores, junto con los importantes cambios que tienen lugar en los primeros años de la adolescencia en el plano psicológico, biológico e interpersonal (Steinberg, 2008), dan lugar a una mayor exposición a situaciones de riesgo (Burén & Lunde, 2018).

Una de estas prácticas de riesgo es el *sexting*, la cual consiste en la creación y envío de mensajes, fotos o vídeos de contenido erótico o sexual a través de Internet o *smartphone* (Barrense-Dias et al., 2017). El *sexting* tiene un importante aumento a medida que los jóvenes se acercan a la adolescencia tardía, pasando del 3 % a los 12 años al 36 % a los 17 (Gámez-Guadix et al., 2017). Los principales motivos por los cuales los adolescentes se inician en esta práctica son la exploración de la sexualidad, la presión social y el deseo de incrementar la autoestima (Alonso Ruido et al., 2017). El *sexting* en si mismo no es peligroso ni constitutivo de delito siempre que se realice de forma consciente y de mutuo acuerdo entre dos o más personas adultas - o menores entre ellos - y con contenido propio o cuya difusión haya sido autorizada previamente por el o los protagonistas. El hecho de que se rompa alguna de las anteriores condiciones resulta en un delito. En caso de difusión del contenido, por parte de uno de los interlocutores o de un tercero, se estará cometiendo un delito de descubrimiento y revelación de secretos tipificado en el Artículo 197.7 del Código Penal[5]. Este es un nuevo tipo penal que fue introducido por la Ley Orgánica 1/2015 de 30 de marzo por la que se modifica la Ley Orgánica 10/1995, en un esfuerzo de la ley por adaptarse a los incesantes cambios que se dan en la sociedad y evitar que numerosos actos delictivos queden sin ser penados por no contemplarse en la legislación. Cabe

[5] Enlace al Artículo 197 del CP: https://www.boe.es/eli/es/lo/1995/11/23/10/con#a197

destacar que en la actualidad esta difusión de contenido suele estar asociada al *revenge porn*, el cual consiste en la publicación en Internet de contenido íntimo con el objetivo de vengarse de una persona, normalmente de la pareja sentimental (Bates, 2017). En caso de que el *sexting* - o la difusión del contenido, tanto propio como ajeno - se de entre un adulto y un menor de edad, se estará cometiendo un delito contra la libertad e indemnidad sexual, tipificado en varios artículos del Título VIII del Código Penal[6], cuyas penas son muy superiores a las recogidas en el Artículo 197.7. La práctica anterior se denomina *grooming* y se define como el proceso por el cual un adulto, mediante el uso de los medios digitales, obtiene material sexual o abusa sexualmente de un menor (Smith & Steffgen, 2013). En España existe una prevalencia de *grooming* entre jóvenes de 12 y 15 años del 15,6 % para las chicas y del 9,6 % para los chicos (de Santisteban & Gámez-Guadix, 2018). Otra consecuencia que puede acarrear el *sexting* es la *sextortion*, que consiste en amenazar a la víctima con revelar imágenes sexuales con el objetivo de forzarla a hacer algo, normalmente enviar más contenido o mantener relaciones sexuales (Patchin & Hinduja, 2020).

El *cyberbullying*, que supone la agresión intencional y repetida que se lleva a cabo en un contexto digital contra aquellos que no pueden defenderse (Hinduja & Patchin, 2008), es otro de los problemas que castigan a la sociedad digital actual, ya que entre un 10 % y un 40 % de la población joven sufre o ha sufrido *cyberbullying* (Garaigordobil, 2015). Diversos estudios han indicado que tanto las víctimas como los propios *cyberbullies* tienen una mayor disposición a sufrir diferentes problemas psicológicos, como puede ser un aumento de los síntomas depresivos, menor autoestima, mayor frecuencia de pensamientos suicidas e incluso de intentos de suicidio (Gámez-Guadix & Gini, 2016). De la misma forma, ambas partes suelen terminar siendo partícipes del *sexting*, buscando en esta práctica una manera de aumentar su autoestima y sentirse socialmente aceptado (Gámez-Guadix & Mateos-Pérez, 2019).

Por si las preocupaciones anteriores no fuesen suficientes, a todo esto se le deben sumar los problemas de adicción a las TIC. Un estudio comprensivo llevado a cabo por el Fondo de las Naciones Unidas para los Niños (UNICEF, 2021), muestra que en Galicia un 59,5 % de los adolescentes son jugadores habituales de videojuegos, de los cuales un 52 % juega a títulos que no son recomendados para su edad. Este estudio muestra que el Pan European Game Information (PEGI[7]), el mecanismo de autorregulación diseñado por la industria para dotar a sus productos

[6] Enlace al Título VIII del CP: https://www.boe.es/eli/es/lo/1995/11/23/10/con#tviii

[7] Enlace a la página web de PEGI: https://pegi.info

de información orientativa sobre la edad adecuada para su consumo, es desatendido tanto por los jóvenes como por sus padres. En promedio los adolescentes gallegos juegan 7,2 horas semanales, pero hay un 4,3 % que les dedica más de 30 horas semanales, algo realmente preocupante. Por otra parte, se estima que más de 3.000 estudiantes de ESO han apostado dinero a través de Internet en alguna ocasión, siendo las apuestas deportivas las más aceptadas (42,6 %). Además de tener un claro componente lúdico y social - lo cual las hace más interesantes -, los jóvenes tienen la creencia de que es fácil ganar dinero apostando en Internet. La Organización Mundial de la Salud (OMS, 2019) tan solo reconoce la adicción al juego y a los videojuegos como las dos únicas Adicciones Sin Sustancia.

En cuanto a los progenitores, son pocos los que ponen límites y normas a sus hijos con respecto al uso de las TIC, reduciéndose el control a la mitad en el segundo ciclo de la ESO y llegando a desaparecer prácticamente en Bachillerato. Esta carencia de supervisión por parte de padres y madres se debe en gran medida al desconocimiento que tiene la población con respecto a los riesgos que existen en Internet y a la importancia de mantener una buena higiene digital en el ámbito familiar (Fundación Barrié, 2022).

El uso problemático de Internet puede llegar a generar un alto grado de interferencia en el día a día de los adolescentes, llegando incluso a convertirse en un problema de salud pública. En Galicia se estima que podría tener una incidencia del 26 %, afectando negativamente a la consolidación de los hábitos de vida saludables, como la alimentación, el sueño o la activad física (Fundación Barrié, 2022). Debido a la alta correlación existente entre los riesgos anteriormente descritos y que la participación de los jóvenes en ellos no para de aumentar (Machimbarrena et al., 2018), resulta crucial desarrollar estrategias de prevención en las que se involucre a todo el sistema educativo (profesorado, familias y adolescentes) para educar en el uso responsable de las TIC, promover programas para la prevención del *cyberbullying* y la adicción y dar el lugar que merece a la educación sexual, donde se debe tratar el *sexting* y sus derivados (Gámez-Guadix & Mateos-Pérez, 2019).

3. Análisis del currículum de la ESO en Galicia

Si se toma en consideración la información presentada anteriormente, parece evidente que la Ciberseguridad es un tema de gran relevancia que debe constituir un motivo de preocupación para la sociedad en su conjunto. El currículum, entendido como "la concreción de los fines sociales y culturales, de socialización que se le asignan a la educación escolarizada" (Gimeno, 1988, p. 15), debe adaptarse a los nuevos retos que supone el avance de las tecnologías. Por lo que con el objetivo de conocer cuál es la importancia y el enfoque que se le da a la Ciberseguridad en el contexto histórico y social actual de la ESO, se ha analizado el Decreto 156/2022, de 15 de septiembre, por el que se establecen la ordenación y el currículo de la educación secundaria obligatoria en la Comunidad Autónoma de Galicia. En el currículum oficial de la ESO en Galicia existen cuatro materias en las que se hace referencia a aspectos relativos a la temática central de este trabajo. Estas materias son:

- Tecnología y Digitalización - Primer curso - Obligatoria
- Tecnología y Digitalización - Segundo curso - Obligatoria
- Educación Digital - Tercer curso - Optativa
- Digitalización - Cuarto curso - De Opción

Todas estas materias inciden de forma directa sobre la Competencia Digital, una de las competencias clave recogidas en el perfil de salida del alumnado al acabar la enseñanza básica previsto por la LOMLOE. De acuerdo con el Decreto anterior (2022):

> La Competencia Digital implica el uso seguro (incluido el bienestar digital y las competencias relacionadas con la Ciberseguridad), saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, para el trabajo y para la participación en la sociedad, así como la interacción con estas. (p. 50064)

Además, también tiene carácter interdisciplinar, ya que contribuye a la consecución de otras competencias clave del perfil de salida, fomentando un aprendizaje permanente y ayudando a crear una ciudadanía digital crítica, informada y responsable que favorezca el desarrollo de la autonomía, la igualdad y la inclusión. Para el desarrollo de la Competencia Digital se trabaja una serie de contenidos relacionados con la Ciberseguridad, los cuales son comunes a las cuatro materias (pp. 50108, 50128, 50447, 50450):

- Seguridad de dispositivos: acciones de configuración específicas. Contraseñas y aplicaciones relacionadas, medidas preventivas y correctivas para hacer frente a riesgos, amenazas y ataques a dispositivos.
- Seguridad en la salud física y mental: medidas de protección de datos e información. Bienestar digital: prácticas seguras y riesgos (ciberacoso, sextorsión, vulneración de la propia imagen y de la intimidad, acceso a contenidos inadecuados, adicciones...).
- Recursos para el tratamiento, la organización la protección de la información y datos personales, de la identidad y de los contenidos digitales.

En cuanto a las líneas de actuación en el proceso de enseñanza y aprendizaje que recoge el Decreto (2022), cabe destacar el uso de metodologías activas con trabajos prácticos en los que se le proporciona autonomía al alumnado a la hora de establecer su propio entorno digital; la utilización de herramientas digitales colaborativas para potenciar las posibilidades que el mundo digital proporciona para el trabajo en grupo, fomentando actitudes participativas y de respeto; la realización de proyectos significativos y la resolución colaborativa de problemas, reforzando la autoestima, la autonomía, la reflexión y la responsabilidad, reduciendo la brecha digital y de género en condiciones de igualdad y por último, el uso responsable, seguro y ético de las tecnologías digitales para aprender a lo largo de la vida y reflexionar de forma crítica sobre la sociedad digital para afrontar situaciones y problemas actuales atendiendo a la diversidad.

Si bien los contenidos que recoge este currículum en materia de Ciberseguridad son correctos, cualquier persona que conozca cómo es la realidad en un centro educativo sabe que es imposible abarcarlos. Estos contenidos forman parte de uno de los múltiples bloques - a su vez repletos de contenidos - de cada materia. Debido a la ingente cantidad de información que se pretende imbuir al alumnado, resulta imposible lograr un aprendizaje situado si el profesorado no media el currículum para dar un peso mayor a la Ciberseguridad. Además, gran parte del profesorado no cuenta con los conocimiento necesarios en este ámbito. No obstante, el Ministerio de Educación y Formación Profesional (2022) ha puesto como objetivo para 2024 que al menos el 80 % de los 700.000 docentes no universitarios acrediten sus competencias digitales en un marco de referencia común a todas las administraciones educativas. Este objetivo se enmarca dentro del Marco Europeo para la Competencia Digital Docente (DigCompEdu), a través del cual se busca dotar a los docentes de las competencias digitales que le permitan aprovechar el potencial de las tecnologías para innovar y mejorar la educación (Vuorikari et al., 2022).

4. Llevando la Ciberseguridad a la ciudadanía

A continuación se analizan algunas de las campañas, servicios y recursos ofrecidos por la Administración Pública para mejorar las competencias en Ciberseguridad de la ciudadanía.

4.1. Campañas

La agenda España Digital 2026[8] es la hoja de ruta para la transformación digital del país, una estrategia que busca aprovechar los beneficios de las nuevas tecnologías para potenciar el crecimiento económico, creando empleo de calidad, con mayor productividad y que contribuya a la cohesión social y territorial. En ella se recogen las estrategias, planes y programas de inversión a seguir para lograr los objetivos establecidos. Una de las tres dimensiones clave de España Digital 2026 es la de las personas, con la que se busca reforzar las competencias digitales de la ciudadanía y garantizar los derechos en el nuevo mundo digital. Para ello, desde las diferentes instituciones públicas se han puesto en marcha numerosas campañas de concienciación y formación. Algunas de ellas se describen a continuación:

• **#ciberprotégete:** El Instituto Nacional de Ciberseguridad de España (INCIBE[9]) presenta la campaña publicitaria #ciberprotégete[10], a través de la cual se trata de concienciar a toda la ciudadanía de la importancia de tomar precauciones en su vida digital. Con ella, el INCIBE recuerda el servicio público Tu Ayuda en Ciberseguridad[11], un servicio nacional, gratuito y confidencial que se pone a disposición de los usuarios de Internet y la tecnología con el objetivo de ayudarles a resolver los problemas de Ciberseguridad que puedan surgir en su día a día. A través de los múltiples canales de comunicación disponibles - teléfono 017, WhatsApp (900 116 117) y Telegram (INCIBE017) - un equipo multidisciplinar de expertos ofrece asesoramiento técnico, psicosocial y legal los 365 días del año a quién lo solicite.

Además, con esta nueva campaña se promueven las guías, los recursos y otras campañas de concienciación[12] lanzadas por la Oficina de Seguridad del Internauta (OSI[13]), uno de los múltiples portales del propio INCIBE.

[8] Enlace a España Digital 2026: https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx
[9] Enlace a la página web de INCIBE: https://www.incibe.es
[10] Enlace a la campaña #ciberprotégete: https://www.incibe.es/ciberprotegete
[11] Enlace al servicio Tu Ayuda en Ciberseguridad: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad
[12] Enlace a las campañas de concienciación de OSI: https://www.incibe.es/ciudadania/formacion/talleres
[13] Enlace a la página web de OSI: https://www.incibe.es/ciudadania

• **Más que un móvil:** A finales de 2022 la Agencia Española de Protección de Datos (AEPD[14]) puso en marcha la campaña Más que un móvil[15], que ofrece a las familias "La guía que no viene con el móvil" (AEPD, 2022b), donde se recogen 10 claves que pretenden ayudar a los padres a la hora de regalar un teléfono móvil a sus hijos. Esta guía hace hincapié en la planificación de la llegada del móvil - debiendo valorar previamente el grado de madurez del menor - y la supervisión, normas y límites que se deben establecer desde un primer momento para que no afecte a otras actividades relevantes de su desarrollo y permita la desconexión digital. Asimismo, manifiesta la importancia de cuidar los datos en redes sociales mediante la correcta configuración de la privacidad del perfil y el deber de concienciar a los menores en no compartir información personal con desconocidos en Internet. Finalmente, la guía anima a los padres a observar la experiencia digital de sus hijos, a prestar ayuda cuando así lo necesiten y a estimular el sentido crítico de los más jóvenes; apelando a la responsabilidad civil de los tutores legales:

> Los padres o tutores legales responden civilmente por los daños y perjuicios materiales y morales causados por las infracciones administrativas o delitos cometidos por sus hijos menores de edad. Asimismo, responden solidariamente de las multas por las infracciones a la normativa de protección de datos impuestas a sus hijos menores de edad y mayores de 14 años. (AEPD, 2022b, clave 8)

Además esta guía cuenta con multitud de enlaces a otros recursos para ayudar a los padres en esta ardua tarea, como la "Guía para padres y profesores" (AEPD, 2022a) o herramientas de control parental[16].

• **Jornadas escolares:** Internet Segura For Kids (IS4K[17]), el Centro de Seguridad en Internet para menores de edad en España, organiza jornadas escolares[18] de carácter gratuito con el objetivo de mejorar las competencias digitales de profesorado y alumnado de Educación Primaria y Secundaria para hacer un uso seguro y responsable de Internet. En estas jornadas se llevan a cabo dos talleres prácticos - dirigidos a alumnado desde 2º de Educación Primaria hasta 2º de Educación Secundaria - donde se busca concienciar a niños y adolescentes sobre los riesgos de Internet y promover buenas prácticas para un uso seguro y responsable del mismo. Por otra parte, el profesorado recibe una sesión de 3 horas en la que se les capacita en la impartición

[14] Enlace a la página web de la AEPD: https://www.aepd.es
[15] Enlace a la campaña Más que un móvil: https://www.aepd.es/es/mas-que-un-movil
[16] Enlace a las herramientas de control parental de IS4K: https://www.incibe.es/menores/familias/control-parental
[17] Enlace a la página web de IS4K: https://www.incibe.es/menores
[18] Enlace a las jornadas escolares de IS4K: https://www.incibe.es/menores/educadores/jornadas-escolares

de unidades didácticas con las que sensibilizar y orientar al alumnado en distintas temáticas sobre el uso seguro y responsable de la Red. Las temáticas de estas jornadas son variadas y el centro escolar puede escoger el tema en función de sus preferencias o necesidades: "Vivimos en Red" (El respeto a los demás y las habilidades sociales para la convivencia en Internet), "Sabes elegir" (La responsabilidad y el espíritu crítico para contrastar información y contactos en redes sociales), "Controla la tecnología" (La protección de dispositivos y servicios *on-line* y otras opciones de seguridad), etc.

4.2. Recursos

Además de la gran cantidad de campañas lanzadas por las instituciones públicas, estas también han creado multitud de recursos para ayudar a la ciudadanía a resolver los problemas cotidianos y a mejorar sus competencias en Ciberseguridad. En esta sección se recogen algunos de los recursos más interesantes y se lleva a cabo una valoración de su utilidad y usabilidad.

• **Avisos de Seguridad:** La Oficina de Seguridad del Internauta (OSI) cuenta con un tablón de anuncios[19] que recoge incidentes que pueden afectar a los usuarios. De cada incidente se indica su fecha de publicación, severidad (Baja - Media - Alta), etiquetas relacionadas y un breve resumen, el cual puede ser ampliado si el lector así lo desea. En este tablón se recogen avisos como: *"La Seguridad Social no ha suspendido tu tarjeta sanitaria, es un smishing"* o *"Campañas de smishing que suplantan la identidad de Correos"*.

Este recurso es verdaderamente útil, pues los anuncios suelen ser publicados el mismo día que comienzan a ocurrir los incidentes. De esta manera, aquellos que consulten este tablón de anuncios diariamente pueden evitar caer en dichas estafas o ataques. Sin embargo, sería más útil si los usuarios se pudiesen suscribir y recibir notificaciones a medida que se publican los incidentes, teniendo información en tiempo real sobre los riesgos que van surgiendo.

• **Canal Prioritario:** La Agencia Española de Protección de Datos (AEPD) ha habilitado un canal prioritario de retirada de contenidos sensibles en Internet[20] para la atención de situaciones delicadas en las que se haya difundido contenido (vídeos o imágenes) de carácter sexual o de agresiones donde se pongan en riesgo los derechos y libertades de los afectados, en especial

[19] Enlace a los Avisos de Seguridad de OSI: https://www.incibe.es/ciudadania/avisos
[20] Enlace al Canal Prioritario de AEPD: https://www.aepd.es/es/canalprioritario

si se trata de menores de edad o víctimas de violencia de género. Cualquier persona, tanto el afectado como un tercero, que tenga conocimiento de la difusión puede acudir a este canal.

Cabe destacar que solo se deberá acudir a este canal prioritario cuando no se haya logrado la retirada del contenido a través de los canales previstos por el prestador de servicios (Google, TikTok, Instagram...) y dicho contenido sea especialmente sensible, ya que de acuerdo con la Razón 18 del Reglamento General de Protección de Datos (RGPD, 2016):

> El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. (pp. 3-4)

Este recurso debería ser conocido por toda la ciudadanía, ya que puede ayudar a preservar la intimidad de las personas afectadas y evitar así que el perjuicio sea aún mayor, tal y como se ha visto la sección Ventajas y malos usos de las TIC e Internet.

• **Juegos educativos:** Entre ellos cabe destacar los juegos de mesa[21] y los recursos interactivos[22] de la OSI y Cyberscouts[23], un conjunto de minijuegos digitales desarrollado por IS4K. Para realizar la valoración de estos juegos interactivos se adoptaron los siguientes criterios:

- Usabilidad: Para ello se han seguido los diez principios de Nielsen (2005).
- Significatividad: Se valorará positivamente el empleo de casos reales.
- Difusión: Se considera indispensable que en estos juegos se presenten al jugador las campañas y servicios que las instituciones públicas ponen a disposición de la ciudadanía.

Si el lector así lo desea puede consultar el análisis completo en el Anexo B - Análisis de los juegos educativos. En resumen, estos juegos cuentan con ciertos aspectos a mejorar. Por ejemplo, ninguno ejemplifica la situación a tratar con casos reales, apenas se proporciona *feedback* al jugador cuando este comete un error y tampoco dan a conocer las campañas, servicios y recursos ofrecidos por las instituciones públicas.

[21] Enlace a los juegos de mesa: https://www.incibe.es/ciudadania/juegos/juegos-mesa
[22] Enlace a los recursos interactivos: https://www.incibe.es/ciudadania/formacion/actividades
[23] Enlace a Cyberscouts: https://www.incibe.es/menores/juegos/cyberscouts

Estudio Empírico

Tras haber llevado a cabo una revisión exhaustiva de los riesgos que acechan a la sociedad digital actual y haber analizado de forma comprensiva la gran cantidad de recursos que la Administración Pública pone a disposición de la ciudadanía, se ha llegado a la conclusión de que el principal problema es el desconocimiento de dichos recursos. Pese a los grandes esfuerzos de la Administración por crear manuales, guías y juegos interactivos, e incluso poner en marcha un servicio como Tu Ayuda en Ciberseguridad, la ciudadanía desconoce casi por completo su existencia. Así lo demuestra el estudio llevado a cabo por el INCIBE (2022b), en el cual se indica que la mitad de los participantes desconoce por completo las campañas sobre Ciberseguridad realizadas por las instituciones públicas. Al centrarse este trabajo en la Educación Secundaria Obligatoria, resultó necesario evaluar de primera mano los conocimientos sobre riesgos básicos, instituciones y campañas que tienen las partes interesadas. Las preguntas de investigación planteadas son las siguientes: ¿Creen que su nivel de conocimiento en Ciberseguridad es adecuado?, ¿Saben definir e identificar algunos de los ataques o riesgos más comunes?, ¿Saben qué implicaciones conlleva el uso del protocolo HTTPS?, ¿Cuántos conocen las instituciones y servicios existentes? y por último, ¿Han surtido efecto las campañas de difusión de la Administración?

1. Método

A continuación se explica el procedimiento metodológico seguido para la realización del estudio. Se trata de una investigación de corte cuantitativo en la cual se emplea un cuestionario *on-line* elaborado *ad-hoc* y validado por una profesora de la Universidad de Santiago de Compostela (Facultad de Ciencias de la Educación) y un profesor de la Universidad de Vigo especialista en Ciberseguridad. En los siguientes apartados se detalla el objetivo del estudio, el instrumento empleado y el procedimiento y la muestra.

1.1. Objetivo

El objetivo principal en el que se centra este estudio es el siguiente:

- ◇ Comprobar el nivel de conocimiento que tiene el alumnado de ESO, profesorado y familias sobre Ciberseguridad: riesgos básicos, instituciones y servicios.

1.2. Instrumento

El instrumento empleado para la recogida de datos fue un un cuestionario *on-line*[24] de carácter cuantitativo. A continuación se analiza cada una de las preguntas de dicho cuestionario:

1. Se solicita a los participantes que se clasifiquen en uno de los 4 grupos que constituyen las partes interesadas:
   a. **Alumnado ESO/Bachillerato:** En este grupo se incluye el alumnado ESO por alusión directa y el de Bachillerato por haber terminado recientemente estos estudios.
   b. **Padres/Madres:** Los progenitores juegan un papel fundamental en la educación digital, por lo que deberían tener una serie de competencias en Ciberseguridad con las que apoyar el desarrollo de sus hijos.
   c. **Profesores:** Al igual que los padres, estos deben tener ciertas competencias que permitan ayudar al alumnado en la formación digital y en la resolución de problemas.
   d. **Otros:** El cuestionario también permite que cualquier persona que no encaje en alguno de los anteriores grupos participe. Es interesante conocer cómo se desenvuelve el resto de la sociedad en este ámbito. En este caso se solicita al participante que introduzca su grupo; por ejemplo, Estudiante universitario, Empleado/a, etc.

2. Se busca conocer cuál es la opinión del participante con respecto a sus competencias en Ciberseguridad, quizás algunos ya saben suficiente o al menos así lo creen.

3. Se pide al participante, en caso de que lo sepa, introducir la institución con la que puede contactar a través del teléfono 017. A través de esta pregunta se puede comprobar si las campañas del INCIBE en las que promocionan este número de teléfono (Tu Ayuda en Ciberseguridad) han surtido efecto en la población. Se espera baja participación.

4. Se pregunta al participante si sabría definir e identificar un ataque de tipo *smishing*, una de las principales estafas en la actualidad. La definición de este término puede ser consultada en el Anexo A - Glosario.

5. Existe la falsa creencia, quizás debida a una mala divulgación de la información por parte de las instituciones o a una comprensión errónea de los conceptos básicos de cifrado, de que cualquier sitio web que cuente con un candado es seguro. El candado indica que se ha emitido un certificado con el cual se cifra la información transmitida entre el sitio

[24] Enlace al cuestionario sobre Ciberseguridad: https://forms.office.com/e/CqWyUjwKt3

web y el internauta a través del protocolo de transferencia HTTPS. No obstante, si la información se transmite a un sitio web fraudulento, de poco sirve que las comunicaciones estén cifradas (OSI, 2020; Ryabova, 2018). La hipótesis planteada asume que la mayoría de los participantes indicarán que la página web SÍ es segura.

6. Se vuelve a evaluar la efectividad de la difusión de la información por parte de la Administración preguntando a los participantes por si han oído hablar del servicio Tu Ayuda en Ciberseguridad. Este es uno de los servicios más importantes que ofrece el INCIBE y el más promocionado. No se espera que muchos encuestados lo conozcan.

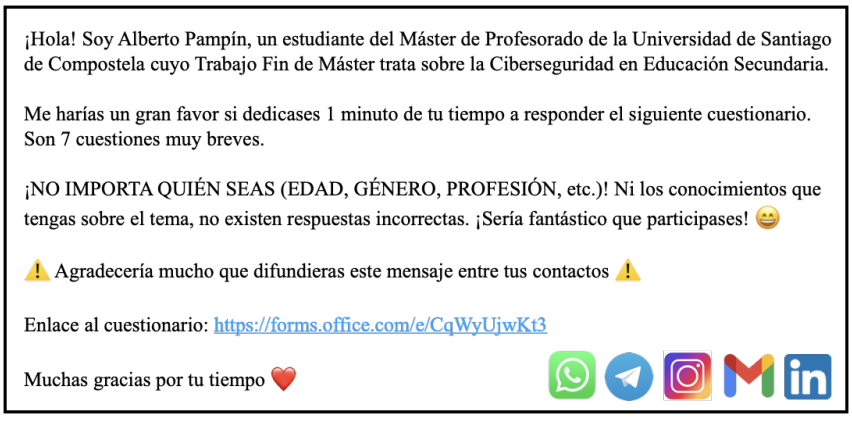
7. Esta última pregunta es muy similar a la anterior, pero se centra en la OSI y sus campañas y recursos. Se presume que un bajo porcentaje de los encuestados la conocerán.

1.3. Procedimiento y muestra

En primer lugar, gracias a la colaboración de la dirección del IES Rosalía de Castro[25], fue posible enviar el cuestionario a todo el alumnado, profesorado y familias del centro. Para ello se utilizó un mensaje muy similar al que se muestra en la Figura 1. En este mensaje se presenta el que suscribe, se destaca el poco tiempo requerido para la respuesta y se invita a cualquier persona a participar, agradeciendo el tiempo dedicado.

Figura 1

Texto utilizado para la difusión del cuestionario



[25] Autorización firmada en Anexo C - Autorización IES Rosalía de Castro

Adicionalmente, para lograr que el cuestionario llegase al mayor número de personas posible se hizo uso de las redes sociales, los mayores canales de difusión actualmente. A través de grupos de WhatsApp y Telegram, Historias de Instagram y Publicaciones en LinkedIn, cientos de personas recibieron de una u otra manera el mensaje de la Figura 1. Tras haber obtenido una gran participación por parte de padres y madres, profesorado y otras personas, se pudo observar que la participación del alumnado era bastante baja, aún habiendo enviado aproximadamente 700 correos. Teniendo en cuenta que gran parte de los estudiantes del segundo ciclo de la ESO no utilizan el correo del centro, se trató de remediar la baja participación mediante la distribución de carteles con un código QR (Anexo C - Figura 19) en el instituto. Al escanear este código QR se puede acceder directamente al cuestionario de Microsoft Forms[26]. Gracias a esta medida y a la ayuda de numerosos profesores del centro la participación del alumnado aumentó de forma significativa.

El cuestionario estuvo activo entre los meses de enero y marzo de 2023. Una vez cerrado, la muestra fue de 1120 personas, la cual será analizada más adelante.

2. Análisis de los resultados

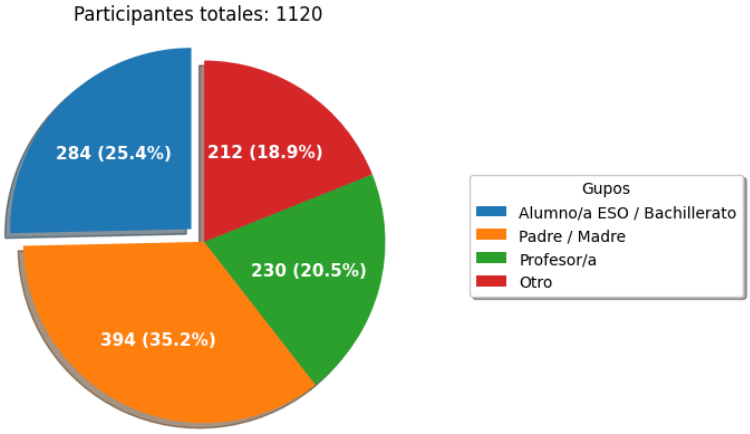
Con el objetivo de optimizar el análisis y divulgación de los resultados, se ha optado por utilizar Jupyter Notebook[27], una aplicación cliente-servidor que permite editar y ejecutar *notebooks* vía navegador web. Un *notebook* es un entorno computacional interactivo diseñado para ayudar a los científicos a trabajar con el lenguaje Python y grandes cantidades de datos, permitiendo incluir código, entradas y salidas de cálculos, imágenes y texto explicativo. Si así lo desea el lector, puede consultar los resultados y el código empleado en este repositorio de GitHub[28].

El número de participantes en el cuestionario fue de 1120, una muestra considerable. En la Figura 2 se puede observar un diagrama sectorial en el que se desglosa la participación atendiendo a los 4 grupos anteriormente citados. Cabe destacar la alta participación de progenitores (35,2 %) y alumnado de ESO y Bachillerato (25,4 %).

[26] Enlace al cuestionario sobre Ciberseguridad: https://forms.office.com/e/CqWyUjwKt3
[27] Enlace a Jupyter: https://jupyter.org
[28] Enlace al repositorio de GitHub: https://github.com/albertopmp/TFM/blob/main/TFM.ipynb

Figura 2

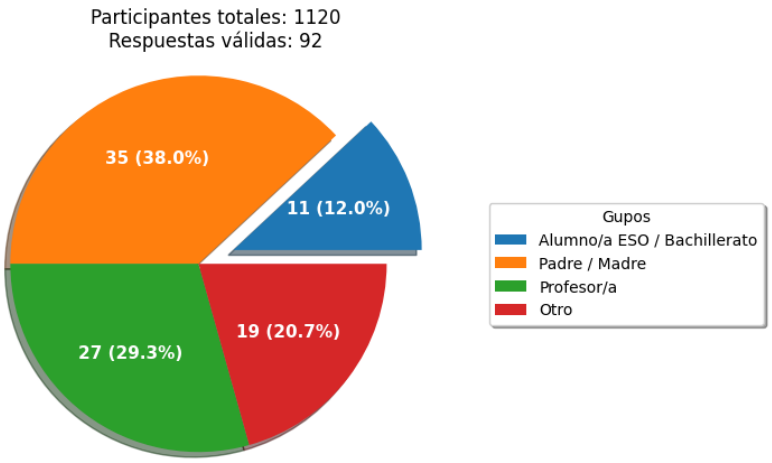
Diagrama sectorial de la participación en el cuestionario



A la tercera pregunta tan solo contestaron 302 (26,96 %) del total de participantes. Una vez descartadas las respuestas sin valor (solo se han dado por buenas las coincidencias “INCIBE” e “instituto”), tan solo 92 (8,21 %) supieron identificar que el 017 es el teléfono de contacto con el INCIBE (Tu Ayuda en Ciberseguridad). Estos resultados verifican la hipótesis expuesta en la sección Instrumento, confirmando que las campañas de difusión de dicha institución no han sido exitosas. En la Figura 3 se puede observar el desglose de los participantes que han respondido correctamente a esta pregunta.

Figura 3

Diagrama sectorial de los participantes que han respondido correctamente a la tercera pregunta



El análisis de la cuarta y quinta pregunta se llevó a cabo mediante el diagrama de barras de la Figura 4. La mayor parte de los encuestados se ven incapaces de definir e identificar un ataque *smishing*. En cuanto al protocolo HTTPS, los resultados sostienen la hipótesis, ya que un gran porcentaje afirma (erróneamente) que una página web con candado sí es segura.

Figura 4

Diagrama de barras para las preguntas 4 y 5

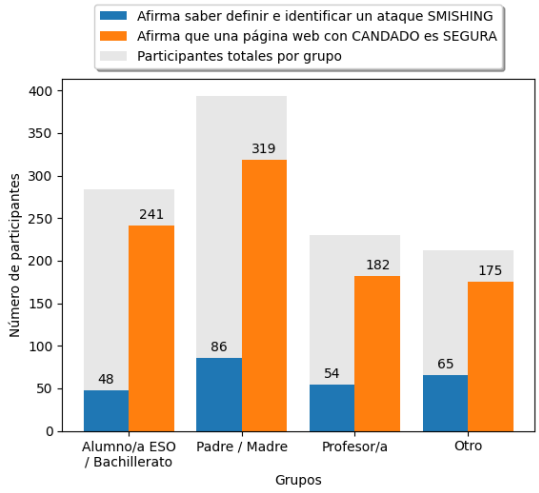
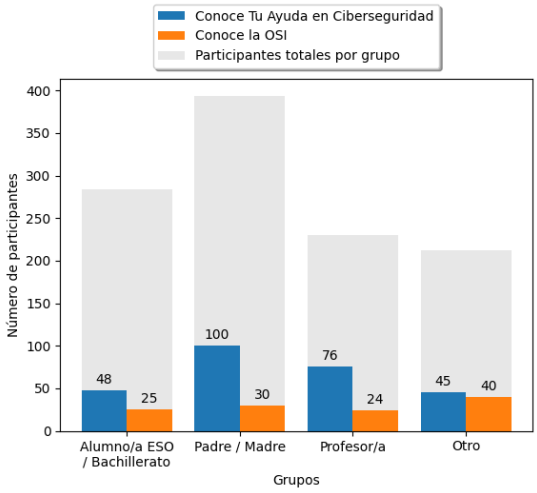


Figura 5

Diagrama de barras para las preguntas 6 y 7



De los 1120 participantes, 242 (21,61 %) afirman saber suficiente sobre Ciberseguridad para resolver cualquier situación en su día a día, según lo indicado en la segunda pregunta. Si se analiza este dato en base a las respuestas que esos mismos participantes han dado a la cuarta y quinta pregunta, se observa que solo 122 (50,41 %) afirman saber definir e identificar un ataque de tipo *smishing* y que 192 (79,34 %) aseguran (erróneamente) que una página web con candado (HTTPS) es segura. Tomando como referencia estos resultados, no parece que sus conocimientos en Ciberseguridad sean suficientes.

Para analizar la sexta y séptima pregunta se elaboró el diagrama de barras de la Figura 5. Los resultados confirman la hipótesis planteada: muy pocos encuestados conocen el servicio del INCIBE o la OSI. Esto evidencia la inefectividad de la difusión llevada a cabo por la Administración. De nada sirve ofrecer servicios y recursos si la ciudadanía ignora su existencia.

Los resultados obtenidos no hacen más que evidenciar la situación de desconocimiento que vive la sociedad actualmente, independientemente del rango de edad o grupo. Las instituciones, junto con los servicios y recursos que ofrecen, suponen una incógnita para la ciudadanía y las campañas que llevan a cabo para darse a conocer no parecen tener el éxito que desearían. Este análisis también revela el desconocimiento de los principales riesgos que existen en Internet.

CYBERTOWN 2D: Material didáctico digital sobre Ciberseguridad

1. Diseño y desarrollo de CYBERTOWN 2D

Tomando en consideración toda la información expuesta en el Marco Teórico y los preocupantes resultados obtenidos a través del cuestionario, resulta evidente la necesidad de un recurso que ayude a la ciudadanía a mejorar sus competencias en Ciberseguridad y que dé a conocer los recursos, instituciones y campañas ya existentes. Por ello, en este trabajo se ha decidido diseñar e implementar desde cero un recurso digital que satisfaga esta imperiosa necesidad. Este recibe el nombre de CYBERTOWN 2D[29]. A continuación, se presentan las motivaciones y decisiones que condujeron a la creación del recurso, desde su concepción inicial hasta su evaluación.

1.1. Proceso de diseño

En esta primera fase, partiendo de los aspectos positivos y aspectos a mejorar de los recursos interactivos desarrollados por la Administración, se definieron las características fundamentales con las que debía contar el nuevo recurso:

- Se deben dar a conocer las instituciones públicas que ofrecen apoyo en Ciberseguridad a la ciudadanía, los servicios disponibles y las campañas y recursos existentes. En decir, todo lo tratado en la sección Llevando la Ciberseguridad a la ciudadanía.
- Los usuarios deben recibir *feedback*. De nada sirve lanzar conceptos de forma desordenada como: *smishing*, *sexting*, nombre de dominio... si no se explica qué son, para qué sirven o cómo pueden protegerse de ellos los internautas.
- Según lo enseñado durante el Máster Universitario en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas, es fundamental conectar con el mundo del alumnado, desarrollando una enseñanza situada a través de prácticas auténticas; es decir, relevantes, significativas en su mundo y cotidianas (Bolivar, 2010). Para ello, los ejemplos que se muestren en el recurso deben ser casos que hayan ocurrido en la realidad.

[29] Enlace al recurso: https://view.genial.ly/6361673e32a5d700111c03ae/interactive-content-cybertown2d

- Resulta indispensable proporcionar al usuario la posibilidad de ampliar la información que se le presenta desde el propio recurso, sin necesidad de buscar en Internet.
- El recurso debe tener una cierta continuidad. Debe existir un hilo conductor u algo que permita trabajar distintos contenidos sin tener que cambiar la dinámica.

A continuación, mediante un proceso de *brainstorming* se plantearon diversas ideas para la jugabilidad y la estética. Finalmente, se decidió crear un recurso interactivo en el que los usuarios tuvieran que moverse por distintas pantallas tomando decisiones y consultando información. En cuanto a la estética, se optó por una similar a la de los juegos clásicos de *Pokémon*: 2 dimensiones (2D) con estilo *Pixel Art*[30]. El lanzamiento del primer juego de *Pokémon* tuvo lugar a comienzos de 1996, hecho que marcó de manera significativa a muchas generaciones, por lo que es muy probable que la familia, el profesorado y el propio alumnado haya tenido exposición directa a dicha estética, lo que puede lograr un mayor *engagement*[31].

En la tercera fase se realizó un análisis de las tecnologías disponibles para la implementación. El resultado de este análisis culminó con dos posibles tecnologías: GDevelop[32] - un motor de videojuegos de código abierto y multiplataforma enfocado al desarrollo de juegos 2D - y Genially [32] - una herramienta *on-line* para crear todo tipo de contenidos visuales e interactivos. Finalmente, Genially fue seleccionada debido a la flexibilidad que ofrece y a las funcionalidades interactivas que ya tiene implementadas. Se optó por descartar GDevelop debido a la curva de aprendizaje que presenta y a la cantidad de tiempo que habría requerido el desarrollo.

Una vez decididas la estética y la tecnología que iban a ser empleadas para el desarrollo, llegó la hora de decidir el contenido a presentar. Este recurso debía servir como medio de divulgación de las propuestas desarrolladas por parte de la Administración Pública, incluyendo:

- **Instituciones:** Instituto Nacional de Ciberseguridad de España (INCIBE), Oficina de Seguridad del Internauta (OSI) e Internet Segura For Kids (IS4K).
- **Campañas:** INCIBE - #ciberprotégete, AEPD - Más que un móvil, IS4K - Jornadas escolares y OSI - Campañas de concienciación.
- **Servicios:** INCIBE - Tu Ayuda en Ciberseguridad, OSI - Avisos de seguridad y AEPD - Canal prioritario de retirada de contenidos sensibles en Internet.

[30] Definición de *Pixel Art*: https://es.wikipedia.org/wiki/Pixel_art
[31] Definición de *engagement*: https://rockcontent.com/es/blog/que-es-engagement
[32] Enlaces a Genially y GDevelop: https://genial.ly/es/, https://gdevelop.io

- **Recursos:** “La guía que no viene con el móvil” (AEPD, 2022b), “Guía para padres y profesores” (AEPD, 2022a) e IS4K - herramientas de control parental.

Por otra parte, fue necesario determinar qué contenido de “carácter técnico” debía ser tratado en el recurso. Para ello se seleccionaron los riesgos más significativos de los expuestos en el Marco Teórico, considerándose estos: el *smishing* y otras técnicas de ingeniería social, las compras *on-line* seguras y los fraudes en Internet, los nombres de dominio y el protocolo HTTPS y, finalmente, el *sexting*, *grooming*, *sextortion* y *cyberbullying*.

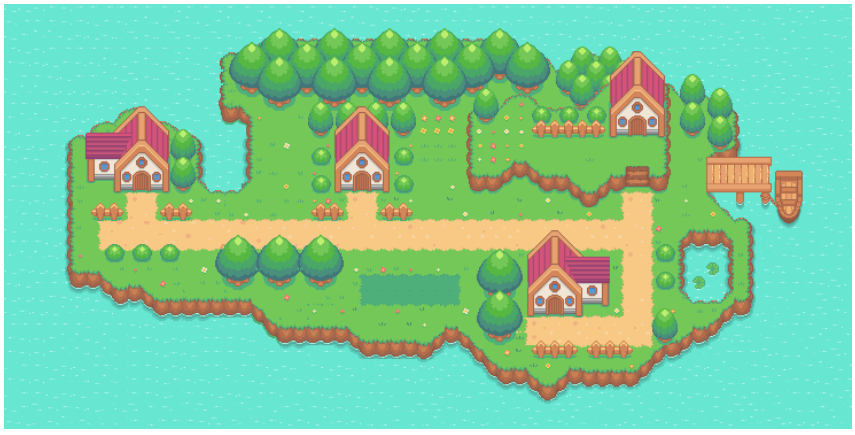
1.2. Desarrollo y descripción de CYBERTOWN 2D

1.2.1. Componentes y Herramientas

Al tratarse de un juego interactivo en 2D, el primer paso consistió en crear el mapa sobre el que se desenvolvería toda la acción. Como base del mapa se empleó el siguiente *tileset*[33, 34] disponible de forma gratuita en Internet y cuyo uso está permitido por el autor. No obstante, con un simple *tileset* no se consigue nada, por lo que fue necesario emplear el *software* Tiled[35] para la creación del mapa. Tras haber comprendido el funcionamiento de esta aplicación, cuya curva de aprendizaje resultó bastante pronunciada, se obtuvo el mapa mostrado en la Figura 6.

Figura 6

Mapa del recurso



Al tratarse de una implementación desde cero (*from scratch*, como se denomina en inglés), también fue necesario diseñar y crear los personajes que darían vida al recurso. En este caso,

[33] Enlace al *tileset*: https://cypor.itch.io/12x12-rpg-tileset
[34] Definición de *tileset*: https://docs.mapbox.com/help/glossary/tileset/

la herramienta utilizada fue Piskel[35], la cual permite al usuario dibujar en estilo *Pixel Art*. El resultado de los personajes se puede apreciar en la Figura 20 del Anexo C. Adicionalmente, se reutilizó una imagen de un loro ya disponible en Internet de manera gratuita y de uso libre. Los personajes dialogan entre ellos y transmiten la información al jugador mediante cuadros de texto o bocadillos de cómic, por lo que para conservar la estética *Pokémon - Pixel Art* fue necesario buscar una fuente de texto acorde. Las fuentes seleccionados fueron: Public Pixel[36] y CC OVERBYTE[37], ambas gratuitas y de uso libre. Si así lo desea el lector, puede encontrar más información sobre las Herramientas y los Recursos empleados en el Anexo C.

1.2.2. Pantallas o Niveles

Para avanzar en el recurso, el jugador pasará por distintas pantallas o niveles en las que tendrá que interactuar con el entorno. Al comienzo se presenta la pantalla de inicio del juego, donde se puede ver el nombre del mismo - CYBERTOWN 2D - y un botón con una animación de pulso que suscita la interacción del usuario (Figura 7).

Figura 7

Pantalla de inicio

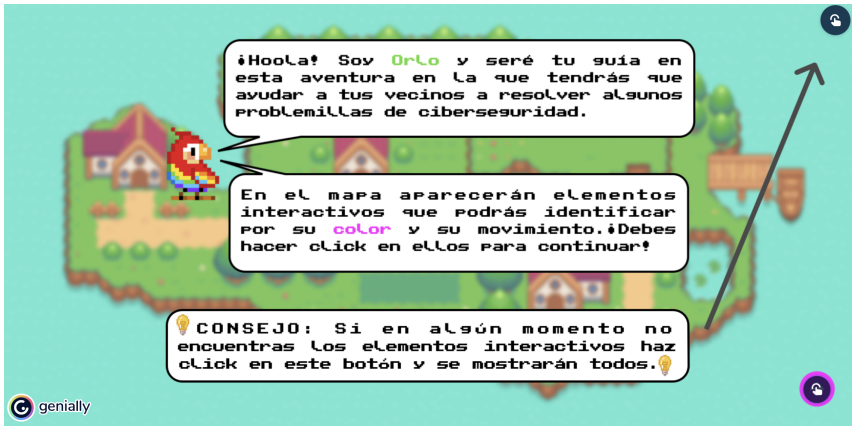
A continuación, el personaje principal - Orlo el loro - presenta el juego e indica al jugador la manera de interactuar: aquellos elementos de color "rosa" (Código HEX #FF00FF) con animación son *clickables*. Este color se utiliza de forma exclusiva para este tipo de elementos y además destaca con respecto al resto de colores, de esta forma se facilita el uso a aquellas personas con algún tipo discapacidad visual. Lo mismo ocurre con las animaciones. También se

[35] Enlaces a Piskel y Tiled: https://www.piskelapp.com, https://www.mapeditor.org
[36] Enlace a Public Pixel: https://www.dafont.com/public-pixel.font
[37] Enlace a CC OVERBYTE: https://www.fontsquirrel.com/fonts/cc-overbyte

indica que el jugador podrá clicar en cualquier momento el botón de la parte superior derecha de la pantalla para visualizar todos aquellos elementos interactivos (Figura 8).

Figura 8

Información sobre la interactividad



A partir de este punto comienza el juego y se irán introduciendo todos los temas comentados en la sección Proceso de diseño. Se han creado tres niveles en los que se tratarán las distintas temáticas. Antes del comienzo de cada nivel se muestra una pantalla en la que se informa al jugador de la temática central y se le da la opción de continuar en este o saltar al siguiente nivel:

■ **NIVEL 1:** El primer nivel trata sobre los ataques de ingeniería social y estafas en Internet. Se presenta al jugador un SMS enviado por el Banco Santander con el siguiente texto: "*Nuevo dispositivo conectado a su banca online, si no reconoce dicha acción verifique inmediatamente: https://santander.login-clientes.com*" (Figura 9).

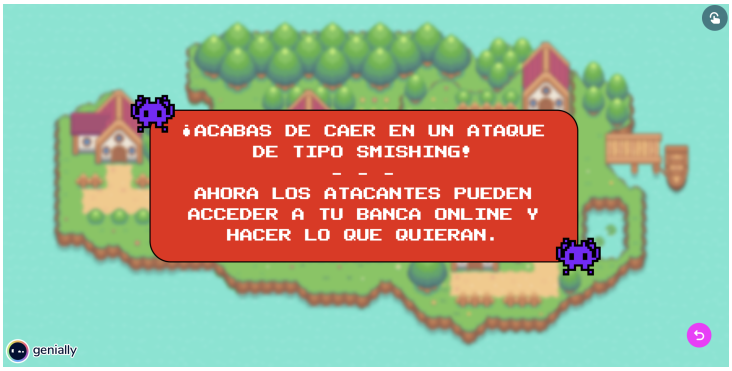
Figura 9

Pantalla inicial del Nivel 1

Uno de los personajes comenta la situación y muestra su preocupación. Por su parte, Orlo indica que existen dos opciones y el jugador debe seleccionar aquella que considere oportuna: la primera implica acceder directamente a la cuenta a través del enlace proporcionado en el SMS para cambiar la clave de acceso y la segunda consiste en analizar con calma la situación, incurriendo en el riesgo de perder definitivamente el control de la cuenta. La forma en la que ambas opciones han sido formuladas incita al jugador a seleccionar la primera. Para muchos la elección será clara y no dudarán en acceder a su cuenta rápidamente; sin embargo, al avanzar, serán sorprendidos con un mensaje que indica que han caído en un ataque de tipo *smishing* y que los ciberdelincuentes podrán acceder con total libertad a su cuentas bancaria (Figura 10)

Figura 10

Pantalla ataque smishing

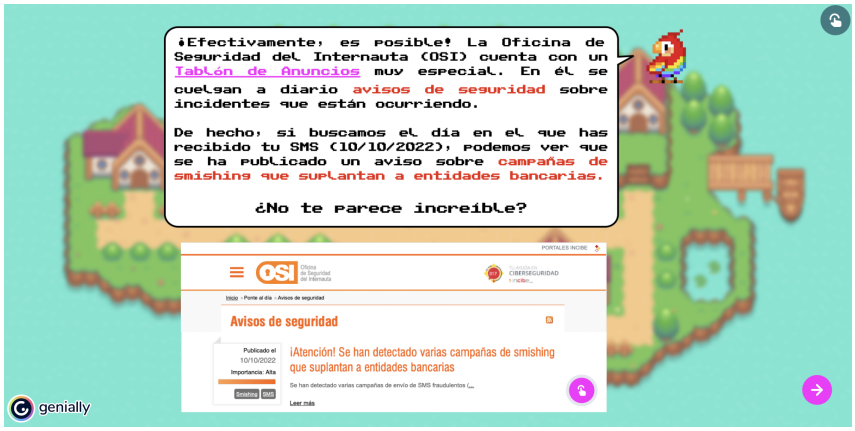


Por suerte, esto es solo un juego educativo y este error no tiene consecuencias. No obstante, en la vida real no aparecerá ningún mensaje que avise del engaño y no habrá una segunda oportunidad, las decisiones erróneas en Internet se pagan muy caras. En este punto, el jugador solo tiene la opción de volver a la pantalla inicial del nivel (Figura 9) y seleccionar la segunda opción. Durante las siguientes pantallas se explica qué son los nombres de dominio y cómo es posible reconocer los ataques de *smishing*, de esta forma el jugador mejora sus competencias en Ciberseguridad aprendiendo habilidades que serán útiles y aplicables en su día a día.

En la penúltima pantalla del nivel (Figura 11) se muestra al jugador una de las herramientas más útiles para poder identificar estos ataques de *smishing*, el tablón de avisos de seguridad de la OSI. Uno de los aspectos a destacar de este SMS es que ha sido recibido por el que suscribe, por lo tanto es un caso real que le podría ocurrir a cualquier persona - característica fundamental de este recurso establecida en la fase de Proceso de diseño. Tanto es así que si se consultan los avisos emitidos por la OSI el día de recepción del mensaje (10/10/2022), se puede observar una alerta de campañas de *smishing* que suplantan a entidades bancarias.

Figura 11

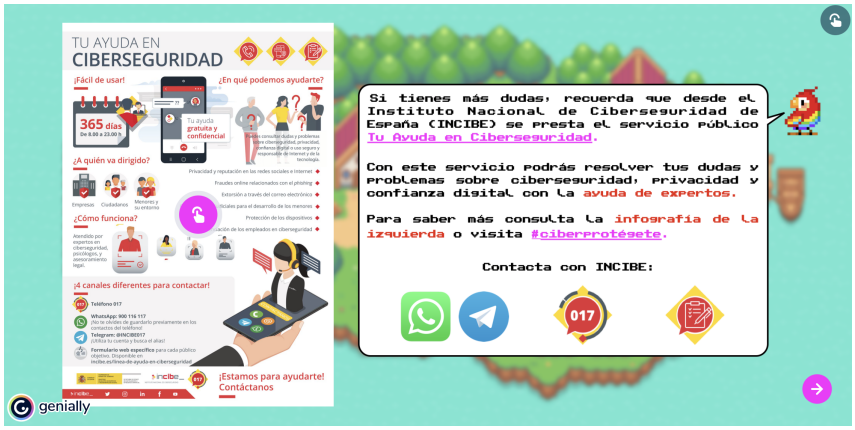
Aviso OSI de campaña de smishing



Por último, se presenta el servicio Tu Ayuda en Ciberseguridad de INCIBE, al cual puede recurrir en caso de necesitar soporte. En pantalla (Figura 12), se muestra una infografía creada por el propio INCIBE donde se amplia información sobre el servicio y a la derecha un bocadillo con enlaces al servicio, a la campaña #ciberprotégete y a los medios de contacto con INCIBE.

Figura 12

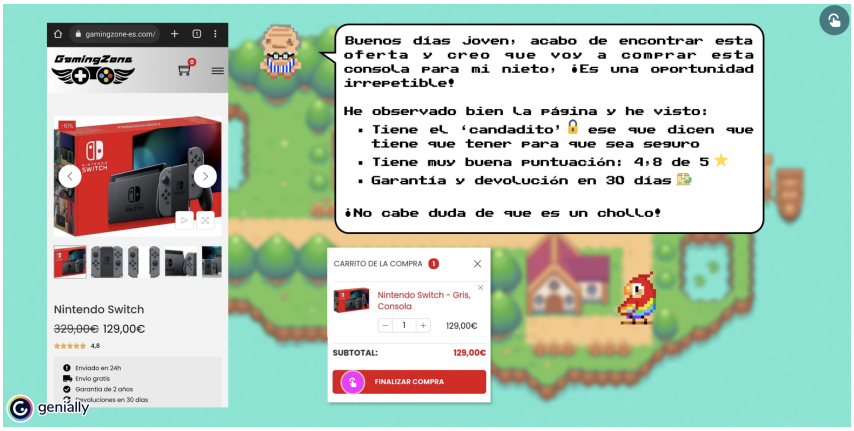
Pantalla Tu Ayuda en Ciberseguridad



■ **NIVEL 2:** La temática de este segundo nivel son las compras *on-line* seguras y los fraudes en Internet. En la Figura 13 se muestra la pantalla inicial de este nivel, donde un abuelo encuentra una gran oferta para comprarle a su nieto la *Nintendo Switch* - una de las consolas de moda en la actualidad - con un descuento de 200€. Además, este personaje lista algunos puntos positivos que ha visto en el sitio web y que ratifican la confianza que deposita en el mismo: cuenta con *"el candadito ese que dicen que es seguro"*, buenas valoraciones, garantía y devolución en 30 días. Al tratarse de una ganga, este entrañable abuelo se dispone a finalizar la compra, pero Orlo lo interrumpe para darle unos consejos sobre Ciberseguridad (Figura 14).

Figura 13

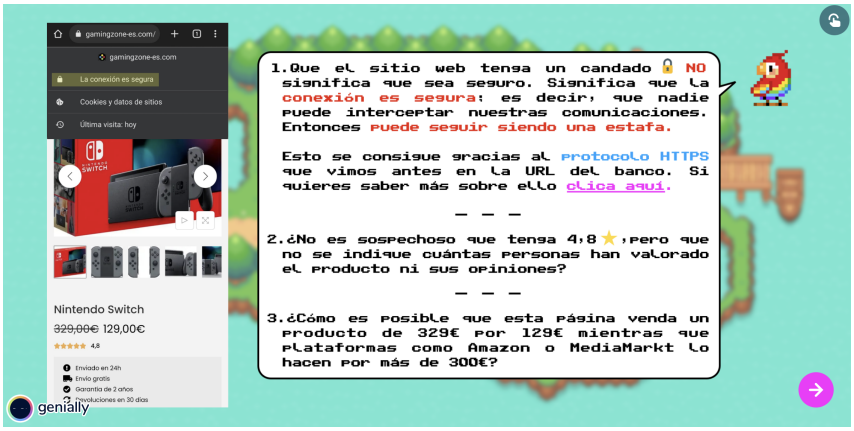
Pantalla inicial del Nivel 2



En primer lugar, se desmitifica la creencia popular de que cualquier página o sitio web que tenga un candado es seguro (Figura 14). Tal y como se ha observado en el análisis de los resultados del cuestionario, existe un gran número de personas que así lo cree. No obstante, el candado solo indica que se utiliza el protocolo de transferencia HTTPS, que implica que las comunicaciones entre internauta y sitio web están cifradas. Si la transferencia de información se realiza hacia un sitio web fraudulento, de poco sirve que esta sea segura (OSI, 2020; Ryabova, 2018). También se comentan algunos otros aspectos que hacen sospechar del sitio web y se indica que es una estafa. A continuación, se muestran dos campañas de la OSI y la "guía sobre compra en segura en Internet" (OSI, 2017) elaborada por la misma institución.

Figura 14

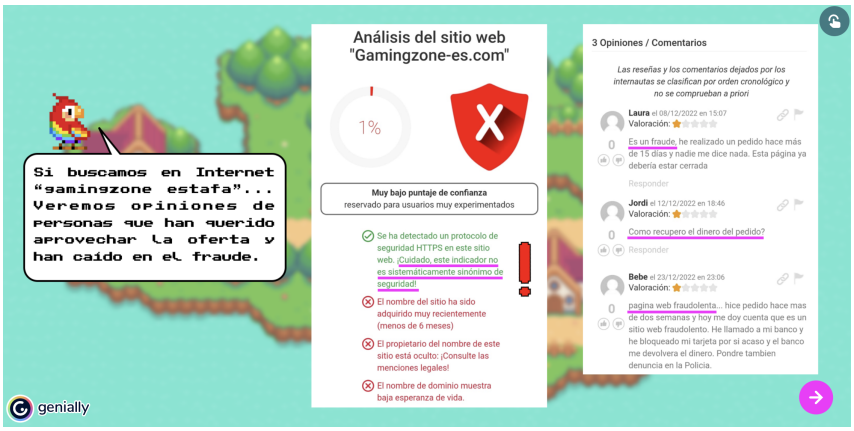
Información sobre sitios fraudulentos



Una vez más, se trata de un caso real. Este sitio web fue creado con motivo del *Black Friday* en noviembre de 2022 para estafar a compradores entusiasmados ante semejante oferta. De hecho, en la pantalla correspondiente a la Figura 15, Orlo muestra que realizando una simple búsqueda en Internet se puede encontrar un análisis de la confianza del sitio web: la puntuación obtenida es muy baja y se explican las razones, indicando que HTTPS (candado) no es sistemáticamente sinónimo de seguridad. También se presentan opiniones de usuarios que han caído en el fraude y desean recuperar su dinero. Normalmente no es posible encontrar análisis de este tipo o comentarios de otros usuarios hasta que ha pasado cierto tiempo desde el comienzo de la estafa, por lo que se recomienda al jugador que en caso de duda haga uso del servicio Tu Ayuda en Ciberseguridad mediante la pantalla de la Figura 12.

Figura 15

Demostración de la estafa



■ **NIVEL 3:** Este último nivel trata sobre el *sexting* y la importancia de la privacidad en Internet. En la pantalla inicial del nivel (Figura 16) se presenta al jugador una conversación entre dos jóvenes en la que comentan las fotos íntimas de una compañera de clase que acaban de recibir y muestran su intención de compartirlas con sus amigos. El guía del juego los interrumpe para impedir que comentan un gran error y darles una lección muy importante.

En la pantalla posterior se explica que la acción que estuvo a punto de cometer es un delito recogido en el Artículo 197.7 del Código Penal. Se hace énfasis en el hecho de que, aunque no haya sido el primero en filtrar el contenido, al formar parte de la cadena de difusión también está cometiendo un delito. A continuación, se define el concepto de *sexting* y se trata de concienciar al jugador de los peligros del mismo con frases como: *"Lo que hoy nos parece un juego, mañana nos puede arruinar la vida"*.

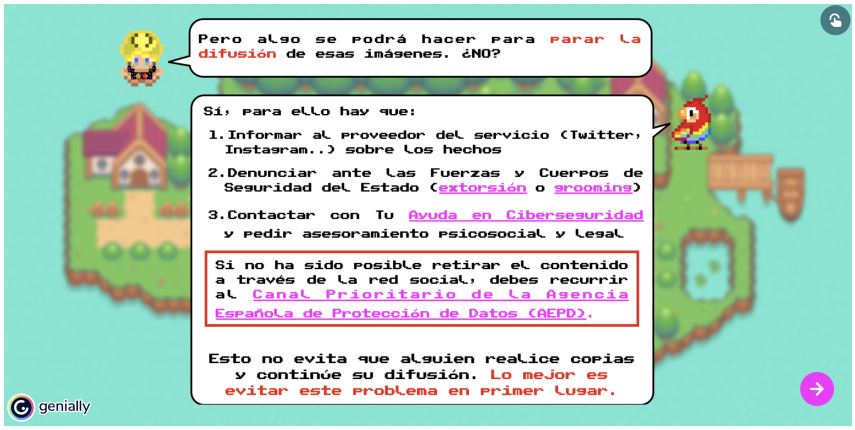
Figura 16

Pantalla inicial del Nivel 3

La pantalla correspondiente a la Figura 17 contiene la forma de proceder en caso de que se produzca una difusión no deseada de contenido íntimo. Se recomienda contactar con el servicio Tu Ayuda en Ciberseguridad y, en caso de no haber sido posible la retirada del contenido a través de la plataforma por la que circula (Twitter, Instagram...), se indica la posibilidad de acudir al Canal Prioritario de la AEPD. Además, se trata de concienciar al usuario insistiendo en que la opción más segura es evitar este problema de raíz y no compartir contenido íntimo, ya que estos medios no evitan que alguien realice copias del contenido y continúe la difusión.

Figura 17

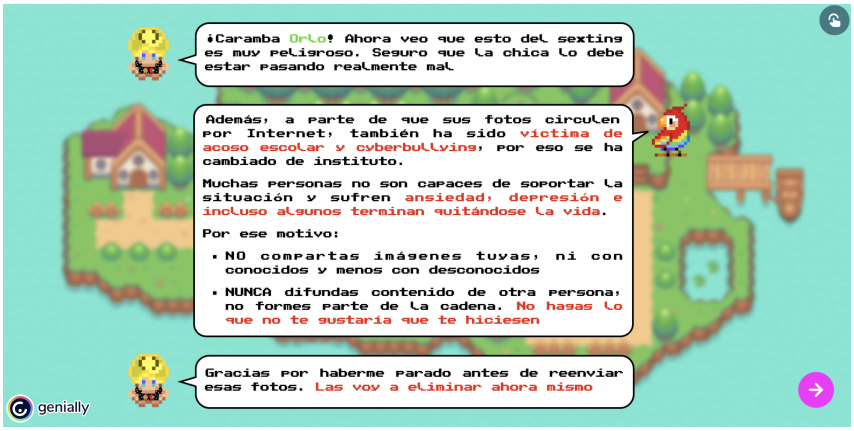
Cómo parar la difusión del contenido



Por último, se presenta la pantalla de la Figura 18 en la que se trata de sensibilizar al jugador de los daños que puede ocasionar la divulgación de contenido sin autorización (ansiedad, depresión e incluso el suicidio) y se pide que no comparta contenido propio ni forme parte de cadenas de difusión: *"No hagas lo que no te gustaría que te hiciesen"*.

Figura 18

Pantalla final de sensibilización



■ **CUESTIONARIO:** Al llegar al final de los niveles el jugador puede responder de forma voluntaria a este cuestionario[38] en el que se valora el recurso: dificultad de uso, conocimiento de los recursos e instituciones presentados, nuevos aprendizajes y utilidad del contenido.

1.2.3. Aspectos relevantes

Durante el desarrollo del recurso se ha cuidado con mucha atención la estética y el diseño de la interfaz de usuario con el objetivo de lograr la mayor usabilidad posible. La usabilidad se define como la facilidad con las que las personas interactúan con una herramienta con el fin de alcanzar un objetivo concreto (Bevan et al., 1991). Para ello se han seguido los diez principios de Nielsen (2005), un gurú de la usabilidad web reconocido en todo el mundo por sus teorías sobre el comportamiento del usuario. Caben destacar las siguientes acciones:

1. Empleo de un color llamativo - "rosa" (Código HEX #FF00FF) - y animaciones para los elementos interactivos con el objetivo de facilitar el uso del recurso, sobre todo a aquellos con alguna discapacidad visual. Lo mismo ocurre con el tamaño de la fuente.
2. Presentación el contenido siguiendo un orden lógico y natural.
3. Diseño estético, atractivo y minimalista.

Tras haber desarrollado la primera versión del recurso, esta se presentó a usuarios pertenecientes a diferentes grupos de edad para comprobar el grado de usabilidad logrado. Tras haber observado con detenimiento la interacción con el juego, se pudo observar que ciertos diálogos y la forma de presentarlos producía cierta confusión. Lo mismo acontecía con algunos elementos

[38] Enlace al cuestionario de valoración: https://forms.office.com/e/8j9MG0dr32

interactivos y otros componentes que buscaban captar la atención de los jugadores. Por consiguiente, se procedió a mejorar dichos aspectos para conseguir una mejor usabilidad.

Otro aspecto fundamental del recurso es el uso del *storytelling* (Starloop Studios, 2022); es decir, el hecho de contar una historia que ayude a los jugadores a mantenerse involucrados en el juego y los motive a entender aquello que están haciendo. También produce esa sensación de continuidad que se estableció como característica en la fase de Proceso de diseño.

2. Evaluación del recurso en un instituto de ESO

Tras completar el desarrollo de CYBERTOWN 2D[39], este estaba listo para ser llevado a un centro de ESO para su evaluación. La evaluación tuvo lugar a finales de abril de 2023 en el IES Rosalía de Castro, dónde ya se había pasado el cuestionario sobre Ciberseguridad. El grupo evaluador estaba formado por 26 alumnos y alumnas de 1º ESO. Se seleccionó este curso puesto que todo el alumnado cuenta con su propio ordenador portátil, gracias al programa E-DIXGAL[40], y su propia cuenta de correo electrónico con acceso a toda la *suite* de Google[41].

El recurso fue presentado por el que suscribe, pero de forma "anónima"; es decir, se eliminaron todas las referencias al autor y se hizo especial hincapié en resaltar que se trataba de un juego publicado en Internet, sin ninguna relación con el autor de este Trabajo Fin de Máster. Este planteamiento pretendía preservar la objetivad del alumnado a la hora de analizar y calificar el recurso, ya que su criterio se vería sesgado en caso de conocer la autoría real. Tras la presentación, el alumnado comenzó a jugar a CYBERTOWN 2D y fue necesaria una sesión de cincuenta minutos para completarlo. Durante esta sesión el que suscribe estuvo presente en el aula, resolviendo las dudas que aparecían y observando el comportamiento del alumnado mientras jugaba, con el objetivo de comprobar si el juego captaba y retenía su atención o si existía alguna dificultad de comprensión debida a la redacción de los diálogos o algún tipo de complicación relativa a la jugabilidad...

En la siguiente sesión, el alumnado comenzó la evaluación del recurso, para la cual se facilitó un Instrumento de evaluación (Anexo C) diseñado *ad-hoc* para la situación. Este documento - al cual pudieron acceder a través de Aula Virtual de la materia de Tecnología y Digitalización

[39] Enlace al recurso: https://view.genial.ly/6361673e32a5d700111c03ae/interactive-content-cybertown2d
[40] Enlace a la página web de E-DIXGAL: http://www.edixgal.com
[41] Enlace a la página web de la *suite* de Google: https://workspace.google.com/intl/es/features/

y copiar a su Unidad de Google Drive - constaba de dos partes:

1. **Análisis**: El alumnado debía responder a una serie de cuestiones relativas al contenido de CYBERTOWN 2D: recursos, instituciones, riesgos... Estas cuestiones fueron utilizadas para evaluar el nivel de conocimiento antes y después de jugar, así como para potenciar la atención del alumnado. Cabe destacar que, en general, el alumnado del IES Rosalía de Castro tiene una gran motivación extrínseca, por lo que cualquier tarea que no lleve asociada una cualificación pasa desapercibida.
2. **Evaluación**: En esta sección el alumnado debía valorar su experiencia con CYBERTOWN 2D: aspectos positivos y aspectos a mejorar, dificultades, errores, método de aprendizaje... También se pide su opinión sobre la importancia que se le da a la Ciberseguridad en la sociedad y en la educación.

Este proceso duró en torno a setenta minutos, repartidos en dos sesiones, durante los cuales el autor de este trabajo estuvo presente en el aula; nuevamente respondiendo dudas y analizando los diálogos del alumnado.

Tras analizar detenidamente los documentos entregados, se ha concluido que la respuesta que CYBERTOWN 2D ha tenido entre el alumnado ha sido fantástica. En el Anexo D - Valoraciones CYBERTOWN 2D se pueden consultar las opiniones de algunos alumnos/as, las cuales se han reiterado en la mayor parte de los documentos. **Tomando sus valoraciones como referencia, parece que CYBERTOWN 2D logra muy satisfactoriamente los objetivos para los que fue diseñado:** consigue captar y retener la atención del alumnado y ayuda a mejorar sus conocimientos en Ciberseguridad, enseñándoles a identificar algunos de los riesgos básicos y dando a conocer las principales campañas, servicios y recursos ofrecidos por la Administración. Entre los aspectos mejor valorados por el alumnado están: la inclusión de casos reales (en especial el de la Nintendo Switch), la explicación de las causas y consecuencias de cada uno de los riesgos y el lenguaje fácil de entender.

De esta evaluación se ha obtenido una información muy interesante, la opinión del alumnado acerca del peso que tiene la Ciberseguridad en la educación. Un número considerable cree que no se le da la importancia que merece y opina que sería necesario dedicar más tiempo del horario lectivo a esta temática.

Conclusiones

A lo largo de este Trabajo Fin de Máster (TFM) se han identificado los principales estudios e investigaciones que analizan el impacto que las TIC e Internet tienen sobre la ciudadanía, prestando especial atención a la adolescencia. La gravedad de la situación descrita por estos estudios ha hecho indispensable el análisis de las medidas que la Administración Pública ha puesto en marcha para proteger y formar a la ciudadanía en materia de Ciberseguridad, por lo que se ha evaluado el currículum de la Educación Secundaria Obligatoria (ESO) en Galicia y se han analizado las principales campañas, servicios y recursos ofrecidos por la Administración. Además, con el objetivo de comprobar el nivel de conocimiento que tiene el alumnado de ESO, profesorado y familias sobre Ciberseguridad, se ha pasado un cuestionario de corte cuantitativo el cual ha sido respondido por 1120 personas. Tras haber tomado en consideración los resultados de los análisis y del cuestionario, se ha desarrollado CYBERTOWN 2D[42], un recurso digital orientado al alumnado de ESO que busca contribuir a la mejora de los conocimientos en Ciberseguridad, el cual está a disposición de los centros educativos y las familias. Además, CYBERTOWN 2D fue llevado a un centro de Educación Secundaria donde ha sido valorado muy positivamente por alumnado de 1º ESO.

De este trabajo se puede concluir que la Ciberseguridad representa y seguirá representado uno de los problemas más relevantes para la sociedad digital. Pese a los notables esfuerzos de las instituciones públicas, ha quedado patente que no son suficientes ni logran los resultados esperados. La ciudadanía desconoce los riesgos a los que se enfrenta e ignora casi por completo sus consecuencias, así como los servicios y recursos que podrían emplear para protegerse. Asimismo, se ha evidenciado que en el ámbito educativo no se le otorga la importancia necesaria. En materia de Ciberseguridad aún queda mucho por hacer, por lo que resulta indispensable seguir trabajando y desarrollando recursos efectivos como CYBERTOWN 2D.

La realización de este TFM ha brindado la oportunidad de poner en práctica y aplicar los conocimientos adquiridos durante el Máster Universitario en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas. A través de él, se ha logrado profundizar de manera significativa en diversos aspectos que conforman la

[42] CYBERTOWN 2D: https://view.genial.ly/6361673e32a5d700111c03ae/interactive-content-cybertown2d

profesión docente, como el análisis de los contenidos curriculares y la comprensión de los desafíos inherentes a la enseñanza en Educación Secundaria Obligatoria. Además, se ha adquirido un mayor conocimiento acerca de las características de los estudiantes, sus contextos sociales y sus motivaciones. En paralelo, la realización de este trabajo ha implicado la búsqueda y el procesamiento de información relevante, con el objetivo de transformarla en conocimiento válido y transferible para su aplicación en procesos de enseñanza-aprendizaje fundamentados en la investigación e innovación educativa.

Aunque CYBERTOWN 2D se considera un éxito por las valoraciones recibidas, habría sido beneficioso contar con un grupo evaluador más amplio con el fin de obtener una mayor cantidad de opiniones y minimizar cualquier sesgo presente. Además, durante el desarrollo de este recurso, se encontraron diversos obstáculos relacionados con la herramienta utilizada. Si bien Genially es una herramienta muy potente que permitió un desarrollo efectivo del recurso, presenta ciertas limitaciones a la hora de implementar "desafíos" o "minijuegos". Por lo tanto, resultaría interesante migrar CYBERTOWN 2D a una nueva plataforma, manteniendo su esencia, pero mejorando la interactividad y añadiendo desafíos que promuevan el aprendizaje y la motivación del jugador. Una vez migrado, sería necesario volver a evaluar el recurso, elaborando un nuevo instrumento de evaluación que contemple estas modificaciones.

A partir de este trabajo se plantean diversas líneas de investigación de especial interés. En los próximos años, se podría analizar si los contenidos introducidos por la LOMLOE en el curso 2022/2023 en relación a la Ciberseguridad son efectivamente incorporados en los centros educativos y si logran generar mejoras significativas en la Competencia Digital del alumnado. Asimismo, sería relevante valorar la efectividad de las nuevas campañas promovidas por la Administración, para comprobar si realmente logran concienciar a la ciudadanía sobre los riesgos y precauciones en el ámbito digital. Por otro lado, sería interesante evaluar el grado de consecución de los objetivos establecidos por el Marco Europeo para la Competencia Digital Docente (DigCompEdu) (Vuorikari et al., 2022), así como las iniciativas impulsadas por el Ministerio de Educación y Formación Profesional. Estas investigaciones podrían proporcionar conocimientos fundamentales para el desarrollo de estrategias educativas y políticas eficaces en el ámbito de la Competencia Digital y la Ciberseguridad.

Bibliografía

Agencia Española de Protección de Datos. (2022a). *Guía para padres y profesores*. https://www.aepd.es/es/documento/guiales-en-internet.pdf

Agencia Española de Protección de Datos. (2022b). *Más que un móvil*. https://www.aepd.es/es/documento/la-guia-que-no-viene-con-el-movil.pdf

Agencia para la Modernización Tecnológica de Galicia. (2016). *Balance Abalar 2010-2014*. https://amtega.xunta.gal/es/documento/balance-abalar-2010-2014

Alonso Ruido, P., Rodríguez Castro, Y., Lameiras Fernández, M., & Martínez Román, R. (2017). Las motivaciones hacia el Sexting de los y las adolescentes gallegos/as. *Revista de Estudios e Investigación en Psicología y Educación*, (13), 047-051. https://doi.org/10.17979/reipe.2017.0.13.2280

Anti-Phishing Working Group. (2022). *Phishing activity trends report*. https://apwg.org/trendsreports

Arango Vila-Belda, J. (1984). El Proyecto Atenea: un plan para la introducción nacional de la informática en la escuela. *Revista de educación*, (276), 5-12.

Barrense-Dias, Y., Berchtold, A., Surís, J. C., & Akre, C. (2017). Sexting and the Definition Issue. *Journal of Adolescent Health*, *61*(5), 544-554. https://doi.org/10.1016/j.jadohealth.2017.05.009

Bates, S. (2017). Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology*, *12*(1), 22-42. https://doi.org/10.1177/1557085116654565

Berners-Lee, T. (2000). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. Harper Business.

Bevan, N., Kirakowski, J., & Maissel, J. (1991). What is Usability? *Elsevier Science*.

Bolivar, A. (2010). *Competencias basicas y curriculo*. Síntesis.

Burén, J., & Lunde, C. (2018). Sexting among adolescents: A nuanced and gendered online challenge for young people. *Computers in Human Behavior*, *85*, 210-217. https://doi.org/10.1016/j.chb.2018.02.003

Caballero, L. (2016). *"Poner negritas era casi un reto": así llegó la informática a los colegios españoles*. https://www.eldiario.es/hojaderouter/tecnologia/informatica-colegios-espana-origen-historia-atenea_1_3737167.html

Decreto 156/2022, de 15 de septiembre, por el que se establecen la ordenación y el currículo de la educación secundaria obligatoria en la Comunidad Autónoma de Galicia. *Diario Oficial de Galicia, 183,* 26 de septiembre de 2022, 50010-50542. (2022). https://www.xunta.gal/dog/Publicados/2022/20220926/AnuncioG0655-190922-0002_es.html

de Santisteban, P., & Gámez-Guadix, M. (2018). Prevalence and Risk Factors Among Minors for Online Sexual Solicitations and Interactions With Adults. *The Journal of Sex Research*, *55*(7), 939-950. https://doi.org/10.1080/00224499.2017.1386763

European Union Agency for Network and Information Security. (2015). *Definition of Cybersecurity*. https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Fondo de las Naciones Unidas para los Niños. (2021). *Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades*. https://www.unicef.es/sites/unicef.es/files/educa/TRIC/Resumen_Ej_TRIC_GALICIA.pdf

Fundación Barrié. (2022). *Adolescencia, Tecnología, Salud y Convivencia*. https://fundacionbarrie.org/prevencion-estudio

Gámez-Guadix, M., De Santisteban, P., & Alcazar, M. (2017). The construction and psychometric properties of the questionnaire for online sexual solicitation and interaction of minors with adults. *Sexual Abuse*, *30*(8), 975-991. https://doi.org/10.1177/1079063217724766

Gámez-Guadix, M., & Gini, G. (2016). Individual and class justification of cyberbullying and cyberbullying perpetration: A longitudinal analysis among adolescents. *Journal of Applied Developmental Psychology*, *44*, 81-89. https://www.sciencedirect.com/science/article/pii/S0193397316300211

Gámez-Guadix, M., & Mateos-Pérez, E. (2019). Longitudinal and reciprocal relationships between sexting, online sexual solicitations, and cyberbullying among minors. *Computers in Human Behavior*, *94*, 70-76. https://doi.org/https://doi.org/10.1016/j.chb.2019.01.004

Garaigordobil, M. (2015). Cyberbullying in adolescents and youth in the Basque Country: prevalence of cybervictims, cyberaggressors, and cyberobservers. *Journal of Youth Studies*, *18*(5), 569-582. https://doi.org/10.1080/13676261.2014.992324

Gimeno, J. (1988). *El currículo: una reflexión sobre la práctica*. Morata.

Hinduja, S., & Patchin, J. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, *29*(2), 129-156. https://doi.org/10.1080/01639620701457816

Instituto Nacional de Ciberseguridad. (2021). *Glosario de términos de ciberseguridad*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Instituto Nacional de Ciberseguridad. (2022a). *Balance de Ciberseguridad*. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

Instituto Nacional de Ciberseguridad. (2022b). *Como se protege la ciudadanía ante los ciberriesgos*. https://observaciber.es/estudios/como-se-protege-la-ciudadania-ante-los-ciberriesgos-abril-2022

International Telecommunication Union. (2021). *Measuring digital development - Facts and Figures*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

Internet World Stats. (2022). *World Internet Users and 2022 Population Stats*. https://www.internetworldstats.com/stats.htm

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Pena. *Boletín Oficial del Estado, 77,* 31 de marzo de 2015, 27061-27176. (2015). https://www.boe.es/eli/es/lo/2015/03/30/1

Machimbarrena, J., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., & González-Cabrera, J. (2018). Internet Risks: An Overview of Victimization in Cyberbullying, Cyber Dating Abuse, Sexting, Online Grooming and Problematic Internet Use. *International Journal of Environmental Research and Public Health*, *15*(11). https://www.mdpi.com/1660-4601/15/11/2471

Ministerio de Educación y Formación Profesional. (2022). *La competencia digital de los docentes será homologable en todo el país*. https://www.educacionyfp.gob.es/prensa/actualidad/2022/06/20220623-sectorial.html

Nielsen, J. (2005). Ten usability heuristics. http://www.useit.com/papers/heuristic/heuristic_list.html

Oficina de Seguridad del Internauta. (2017). *Compra segura en Internet - Guía Práctica*. https://www.osi.es/sites/default/files/docs/guia_compra_segura_internet_web_vfinal.pdf

Oficina de Seguridad del Internauta. (2020). *HTTPS y certificados digitales, ¿me debo fiar de todos?* https://www.osi.es/es/actualidad/blog/2020/07/27/https-y-certificados-digitales-me-debo-fiar-de-todos

Oficina de Seguridad del Internauta. (2021). *Guía de ciberataques*. https://www.osi.es/es/guia-ciberataques

Organización Mundial de la Salud. (2019). *Addictive behaviour*. https://www.who.int/health-topics/addictive-behaviour

Patchin, J., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse*, *32*(1), 30-54. https://doi.org/10.1177/1079063218800469

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). *Diario Oficial de la Unión Europea, 119,* 4 de mayo de 2016. (2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

Rodríguez Rodríguez, J., & Losada Loureiro, C. (2019). Análisis del Proyecto de Educación Digital (E-DIXGAL): la visión del profesorado de Educación Primaria. *Digital Education Review*, (36), 171-179. https://doi.org/10.1344/der.2019.36.171-189

Ryabova, Y. (2018). *El protocolo HTTPS no garantiza la seguridad*. https://www.kaspersky.es/blog/https-does-not-mean-safe/15135/

Smith, P., & Steffgen, G. (2013). *Cyberbullying through the new media : findings from an international network*. Psychology Press.

Starloop Studios. (2022). *How to Use Storytelling and Transmedia in Video Games?* https://starloopstudios.com/how-to-use-storytelling-and-transmedia-in-video-games/

Steinberg, L. (2008). A social neuroscience perspective on adolescent risk-taking. *Developmental Review*. https://doi.org/10.1016/j.dr.2007.08.002

Vallejo, S. (2022). 600 trabajadores públicos de Granada 'pican' en un simulacro de estafa por 'phishing'. *Granada Hoy*. https://www.granadahoy.com/granada/Experimento-Ayuntamiento-Granada-pishing-secuestro-correos_0_1738926428.html

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes. *Publications Office of the European Union*. https://doi.org/10.2760/115376

Xunta de Galicia. (2022). *Actualización do repositorio de contidos de espazoAbalar con 46 novos recursos educativos dixitais*. https://www.edu.xunta.gal/espazoAbalar/es/noticia/actualizacion-do-repositorio-de-contidos-de-espazoabalar-con-46-novos-recursos-educativos

Xunta de Galicia. (2023). *La Xunta abre el plazo para incorporar 25 nuevos centros al programa de libro electrónico E-Dixgal*. https://www.xunta.gal/notas-de-prensa/-/nova/77657/xunta-abre-plazo-para-incorporar-25-nuevos-centros-programa-libro-electronico?langId=es_ES

Zakon, R. (2018). *Hobbes' Internet Timeline 25*. https://www.zakon.org/robert/internet/timeline

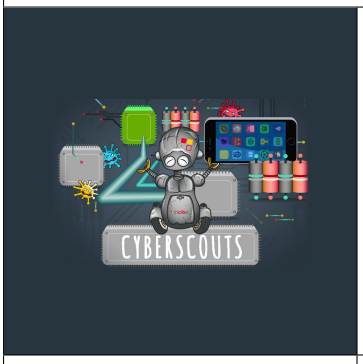
Anexo A - Glosario

En el ámbito de la informática se utiliza una gran cantidad de palabras compuestas y anglicismos, los cuales no suelen tener una traducción directa al español o, si esta existe, no se utiliza frecuentemente. En esta sección se recogen, en orden alfabético, las definiciones de algunos términos que han sido utilizados a lo largo de este documento:

- ***Adware*:** Software que se apoya en anuncios (normalmente para financiarse) como parte del propio programa. En algunos casos se les considera *malware*. Común en las versiones gratuitas en las aplicaciones (OSI, 2021)
- **Ciberataque:** Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente danos al sistema (INCIBE, 2021)
- ***Cyberbullying*:** Supone la agresión intencional y repetida que se lleva a cabo en un contexto digital contra aquellos que no pueden defenderse (Hinduja & Patchin, 2008)
- **Ciberseguridad:** Referente a la seguridad del ciberespacio, donde este último se considera el conjunto de conexiones y relaciones entre objetos que son accesibles a través de la red generalizada de telecomunicaciones, y al conjunto de objetos que pueden ser controlados de forma remota o cuyos datos pueden ser accesibles de manera remota (ENISA, 2015)
- ***Grooming*:** Proceso por el cual un adulto, mediante el uso de los medios digitales, obtiene material sexual o abusa sexualmente de un menor (Smith & Steffgen, 2013)
- **Ingeniería social:** Conjunto de técnicas utilizadas por los ciberdelincuentes para engañar a los usuarios de sistemas/servicios TIC con el objetivo de que estos faciliten datos de valor, ya sean credenciales, información sobre los sistemas, servicios instalados, etc. (INCIBE, 2021)
- ***Malware*:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: *malicious software* (INCIBE, 2021)

- ***MFA (Multi Factor authentication)*:** También conocida como autenticación en dos pasos o factores, agrega una capa de protección al proceso de inicio de sesión. Al acceder a una cuenta o aplicación, el usuario debe pasar por una verificación de identidad adicional; por ejemplo, tiene que escanear su huella digital o especificar un código que recibe en su teléfono (OSI, 2021)
- ***Pan European Game Information* (PEGI):** El mecanismo de autorregulación diseñado por la industria del videojuego para dotar a sus productos de información orientativa sobre la edad adecuada para su consumo
- ***Phishing*:** Ciberataque de ingeniería social en el que se suplanta a una entidad o servicio mediante un email, RRSS, llamada telefónica (*Vishing*) o mensaje SMS (*Smishing*) para conseguir credenciales o información de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo (INCIBE, 2021; OSI, 2021)
- ***Ransomware*:** Malware cuya funcionalidad es "secuestrar" un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella (INCIBE, 2021)
- ***Revenge porn*:** Práctica de riesgo en Internet que consiste en la publicación de contenido íntimo de una persona con el objetivo de vengarse de ella, normalmente la pareja sentimental (Bates, 2017)
- ***Sexting*:** Consiste en la creación y envío de mensajes, fotos o vídeos de contenido erótico o sexual a través de Internet o *smartphone* (Barrense-Dias et al., 2017)
- ***Sextortion*:** Práctica de riesgo en Internet que consiste en amenazar a la víctima con revelar imágenes sexuales con el objetivo de forzarla a hacer algo, normalmente enviar más contenido o mantener relaciones sexuales (Patchin & Hinduja, 2020)
- **TIC:** Tecnologías de la Información y la Comunicación

Anexo B - Análisis de los juegos educativos

<table>
<tr><td colspan="2">Cyberscouts</td></tr>
<tr><td> 
</td><td>Descripción oficial: Cyberscouts ofrece a niños y adultos varios minijuegos a través de los cuales adquirir conocimientos para hacer un uso más seguro de los servicios de Internet. Entre los minijuegos disponibles se encuentran: Sopa de letras, Juego de diferencias, Busca lo malo... Cada uno de ellos tiene una jugabilidad distinta y aporta diferentes aptitudes al jugador.</td></tr>
<tr><td>Aspectos Positivos</td><td>■ Es una buena herramienta para reforzar conceptos, no para adquirirlos, tal y como se promete en su descripción.
■ Jugabilidad e Interacción Persona-Ordenador interesante.
■ Variedad de minijuegos y conceptos.</td></tr>
<tr><td>Aspectos a Mejorar</td><td>■ Muchos de los minijuegos no son prácticas auténticas; es decir, relevantes, significativas en el mundo de los usuarios y cotidianas. No se utilizan casos reales, son simulaciones.
■ En numerosas ocasiones solo se lanzan conceptos o vocablos a los usuarios para que los clasifiquen o hagan algo con ellos, pero sin dar ninguna información sobre ellos.
■ No hay feedback para las respuestas correctas/incorrectas.
■ Imposibilidad de acceder a más información u otros recursos sobre la materia correspondiente desde el propio juego.</td></tr>
</table>

Juegos de mesa	
	**Descripción oficial:** Serie de juegos de mesa que los usuarios deben descargar e imprimir. Estos juegos están pensados para ser jugados en familia o con amigos y existen diversas temáticas como: Gestión y Ciberseguridad, Trivial, Quién es quién...
Aspectos Positivos	▪ Contiene soluciones con explicaciones para poder comprender mejor por qué la opción escogida es correcta/incorrecta. ▪ Interesante para pasar un buen rato en familia y aprender. ▪ Estética y jugabilidad original.
Aspectos a Mejorar	▪ La necesidad de imprimir los juegos y montar tablero y piezas hace que mucha gente no esté interesada en ellos. ▪ Requiere que se juegue en grupo y que todos los integrantes estén atentos e interesados. ▪ Imposibilidad de acceder a más información u otros recursos desde el propio juego al ser en formato físico.

Recursos interactivos	
	**Descripción oficial:** Serie de recursos pedagógicos interactivos para que los usuarios comprueben y protejan la información que comparten, detecten situaciones de riesgos y analicen los permisos que conceden a las diferentes apps que descargan.
Aspectos Positivos	▪ Son prácticas auténticas; es decir, relevantes, significativas en el mundo de los usuarios y cotidianas. ▪ Presentan al usuario situaciones en las que deben elegir entre dos opciones, buscando cierto choque cognitivo. ▪ Ofrecen feedback al usuario y se le presentan enlaces a otros recursos/contenidos relevantes.
Aspectos a Mejorar	▪ Son recursos aislados, no están relacionados de ninguna manera por lo que el usuario debe entrar y salir a cada uno. Sería más interesante que hubiese cierta continuidad.

Anexo C

1. Cartel con código QR

Figura 19

Cartel con código QR

CUESTIONARIO SOBRE CIBERSEGURIDAD

6 PREGUNTAS BREVES - 1 MINUTO

♡ GRACIAS POR PARTICIPAR ♡

Alberto Pampín - Exalumno IES Rosalía de Castro
Trabajo Fin de Máster - Máster de Profesorado USC

2. Autorización IES Rosalía de Castro

Eu, **D. XAVIER MOURIÑO CAJIDE,** coma **DIRECTOR** do **IES Plurilingüe Rosalía de Castro**, **AUTORIZO** a **D. ALBERTO PAMPÍN PÉREZ** a **citar o nome do centro** no seu **Traballo Fin de Máster** do Máster Universitario en Profesorado de Educación Secundaria Obrigatoria e Bacharelato, Formación Profesional e Ensinanzas de Linguas, con motivo do **cuestionario sobre Ciberseguridade e da proposta de recurso dixital** levados a cabo no centro.

Asinado:

35281759N JAVIER MOURIÑO (R: Q6555198H)

Firmado digitalmente por 35281759N JAVIER MOURIÑO (R: Q6555198H)
Fecha: 2023.05.24 12:58:37 +02'00'

D. XAVIER MOURIÑO CAJIDE

3. Herramientas

- Creación del juego: Genially
- Creación del mapa: Tiled
- Creación de *sprites*: Piskel
- Edición de imágenes: PhotoScape
- Composición de diálogos e imágenes: Numbers

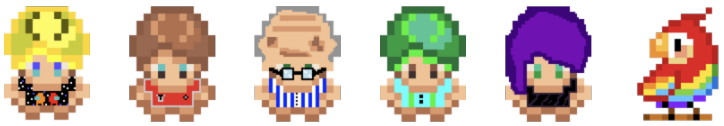
4. Recursos

- Tileset
- Parrot
- Emoji Virus
- Emojis Apple
- Fuente Public Pixel
- Fuente CC OVERBYTE

5. Personajes CYBERTOWN 2D

Figura 20

Personajes CYBERTOWN 2D



6. Instrumento de evaluación

CYBERTOWN 2D IES Rosalía de Castro

Análisis de CYBERTOWN 2D

Utiliza esta plantilla para tu análisis

Nombre y Apellidos:
Curso:

Anota los **recursos e instituciones** sobre los que habla el juego. Añade tantos elementos a la siguiente lista como creas necesario:

-
-
-

¿Cuántos de ellos conocías antes de jugar? Marca los que ya conocías en rojo

¿Crees que alguno de ellos será útil para tu día a día? ¿Por qué?

-

¿Habías consultado alguna de estas webs antes? ¿Para qué?

-

Anota los **riesgos y peligros** que trata CYBERTOWN 2D. Añade tantos elementos a la siguiente lista como necesites. Además, **define cada uno de ellos** (utiliza la información del juego y los enlaces presentados):

-
-
-

¿Cuántos de ellos conocías antes de jugar? Marca los que ya conocías en rojo

Si alguno de ellos te hubiese ocurrido en la vida real antes de jugar CYBERTOWN 2D, ¿crees que habrías sido capaz de identificarlo? **Explica el motivo de tu respuesta**

-

¿Crees que **con lo que has aprendido en este juego sabrías identificar alguno** de estos riesgos y peligros? Indica al menos uno y describe cómo actuarías

-

¿Conoces algún caso cercano que haya sufrido las consecuencias de estos riesgos? Si esa persona ha sido capaz de identificar el riesgo y evitarlo indica cómo lo hizo. En caso contrario, indica cómo actuarías tú

-

¿Qué es un nombre de dominio? ¿Y un subdominio? Pon ejemplos que reales que ilustren tu explicación. Intenta que no sea el mismo ejemplo que aparece en el juego 😉

-

Valoración de CYBERTOWN 2D

Utiliza esta plantilla para tu valoración

¡Completa esta parte solo cuando hayas terminado de jugar y completado el análisis!

¿Crees que es posible jugar y aprender a la vez? ¿Prefieres aprender así o con un método más tradicional? **Justifica tu respuesta**

-

¿Te ha resultado difícil entender los conceptos que trata el juego? ¿Qué es lo que te ha parecido más difícil? ¿Por qué?

-

¿Ha sido fácil interactuar con el juego? Indica si te has quedado bloqueado en algún momento o si has tenido algún problema (indica en qué parte del juego)

-

¿Qué consideras que se podría cambiar en CYBERTOWN 2D para mejorarlo?

-

¿Qué es lo que más te ha gustado de CYBERTOWN 2D?

-

¿Crees que la sociedad le da la importancia que merece a la Ciberseguridad? **Explica**

-

¿Opinas que en los colegios e institutos se enseña suficiente sobre Ciberseguridad? ¿Ha sido esta la primera vez que has recibido formación sobre este tema? **Explica**

-

Anexo D - Valoraciones CYBERTOWN 2D

A continuación se muestran algunas de las valoraciones realizadas por el alumnado:

- *"El riesgo más difícil de identificar creo que fue el smishing, en el juego fallé la primera vez y no hubiera sabido como actuar ni como identificarlo.* ***Ahora sé cómo comprobar si una página es segura o real y cómo actuar****."*
- *"Me ha gustado que* ***los casos tratados son reales****, por ejemplo la estafa de la Nintendo Switch, ya que en gente de nuestra edad es normal querer comprar una consola, por lo que es más probable que nos ocurra."*
- *"****Me sorprendió toda la cantidad de información que fui capaz de aprender en tan poco tiempo y solo jugando a un juego****. Tengo bastante claro que si hubiera tenido que aprender todo esto de forma tradicional hubiera tardado muchísimo más."*
- *"Lo que más me ha gustado sobre el juego es que* ***te explica un montón de cosas, pero lo hace bien****.* ***El lenguaje que usa se puede entender de manera muy fácil y resume muy bien la informació****n. Es decir, te cuenta solo lo necesario, así aprendes mucho y no te lías con datos innecesarios que solo van a complicar más el juego."*
- *"Lo que más me ha gustado de CYBERTOWN2D es que* ***explica muy bien todas las causas y consecuencias de cada uno de los casos que trata****. Además lo hace de una forma fácil y divertida."*
- *"****En mi opinión no se da la importancia que merece a la Ciberseguridad.*** *El claro ejemplo está en que es un tema muy importante sobre el que nunca nos habían informado el colegio.* ***Gran parte de la población se toma esto como una broma*** *y creen que son tonterías, en vez de abrir los ojos y ver que es un tema serio que nos afecta a todos."*
- *"Considero que los centros informan muy poco sobre esto, deberían hacerlo mucho más.* ***Me perecería muy buena idea que en todos los centros se utilizase una hora de clase para informar sobre este tema****. Incluso estaría bien que se hicieran pruebas prácticas, para ver si sabríamos reaccionar correctamente ante situaciones como estas."*
- *"Creo que no se enseña lo suficiente. Esta ha sido la primera vez que tengo una charla de Ciberseguridad,* ***por lo que en los colegios se le da muy poca importancia. Incluso creo que se le debería de dedicar una hora como mínimo a la semana****."*