Universidad Internacional de La Rioja
Facultad de Educación

Máster Universitario en Tecnología Educativa
y Competencias Digitales

"Exploit City": Gamificación como método de adquisición de conductas seguras en la red

Trabajo fin de estudio presentado por:	Alejandro Dayekh García
Tipo de trabajo:	Proyecto de Innovación
Director/a:	Noemí Suárez Monzón
Fecha:	30/06/21

Resumen

"Exploit City" es una propuesta de gamificación que tiene el objetivo de dotar a preadolescentes de conocimientos y procedimientos en seguridad en la red. Los fundamentos teóricos, que sustentan su aplicación, se basan en la necesidad de aplicar una metodología emergente de carácter lúdico para introducir en la enseñanza las múltiples amenazas propias del mundo de la ciberdelincuencia en internet, ahondando también en el sector de las redes sociales. Dichas premisas estarán sustentadas en base a distintos datos estatales, los cuales dejarán clara la necesidad de informar a los menores de los posibles riesgos que pueden afrontar en sus primeros dispositivos tecnológicos. El diseño de la propuesta didáctica se basará en la implementación de una experiencia gamificada en una ciudad futurista del siglo XXIII. El alumnado realizará su avance educativo habitual por medio de actividades desarrolladas con recursos basados en situaciones simuladas. Todo este planteamiento estará dotado de múltiples elementos, componentes y estéticas únicas del espacio gamificado. Esta experiencia se presentará a dos sectores profesionales para su evaluación. Concretamente, será valorada por dos docentes y un experto policial en ciberdelincuencia. Estas valoraciones serán contrastadas con una autoevaluación del autor, lo cual facilitará el desarrollo objetivo de las conclusiones del proyecto.

Palabras clave: Gamificación, ciberseguridad, redes sociales, peligros

Abstract

"Exploit City" is a gamification proposal that aims to provide pre-teens with knowledge and procedures in network security. The theoretical foundations, which support its application, are based on the need to apply an emerging methodology of a playful nature to introduce into teaching the multiple threats typical of the world of cybercrime on the internet, also delving into the social network´s sector. Said premises will be supported on the basis of different state data, which will make clear the need to inform minors of the possible risks they may face in their first technological devices. The design of the didactic proposal will be based on the implementation of a gamified experience in a futuristic city of the XXIII century. Students will carry out their usual educational progress through activities developed with resources based on simulated situations. All this approach will be endowed with multiple elements, components and unique aesthetics of the gamified space. This experience will be presented to two professional sectors for evaluation. Specifically, it will be assessed by two teachers and a police expert in cybercrime. These evaluations will be contrasted with a self-evaluation of the author, which will facilitate the objective development of the project's conclusions.

Keywords: Gamification, cybersecurity, social networks, dangers

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

El tópico seleccionado para el Trabajo de Fin de Máster realmente se encuentra diversificado en tres líneas temáticas que creo indisolubles a la hora de abordar el diseño didáctico. Dichos temas son la gamificación, la ciberseguridad y las redes sociales. Cabe decir que los dos últimos mencionados han ganado notoriedad con el avance tecnológico. Esto ha captado el interés de muchos agentes investigadores de todas las esferas investigativas, incluidas las del campo educativo. De hecho, la propuesta de este trabajo pretende presentar a un alumnado de sexto curso de primaria estas dos realidades intangibles y complejas (ciberseguridad y redes sociales) a través de la metodología de gamificación.

1.1. Justificación y planteamiento del tema elegido

Teniendo que fundamentar el papel de la gamificación en este proyecto, es primordial entender que "el juego es una actividad intrínsecamente motivadora en la que nos involucramos por puro placer" (Valderrama, 2015, p.75). En otras palabras, si es necesario lograr que el alumnado aprenda por placer, relacionando los contenidos curriculares que aprende a momentos positivos y divertidos (una expresión más del aprendizaje significativo), cobra más relevancia buscar este modo de motivación en procedimientos complejos y abstractos. Dentro de dichos procesos, sin duda, pueden localizarse los relacionados con la ciberseguridad y las redes sociales. En futuros puntos podrá visualizarse claramente el carácter "manipulador" que tiene la gamificación gracias al efecto lúdico de la misma, pero ahora tiene prioridad comentar los motivos técnicos y las experiencias observables que corroboran el peligro de los dos frentes virtuales de la propuesta.

Por un lado, adentrándose en la importancia de modificar las malas praxis de los niños y niñas en la red, puede comprobarse, gracias a datos del Instituto Nacional de Estadística (INE) del año 2020, que el 68,8% de los menores de 12 años ya disponían de un móvil. De hecho, en esta misma edad, los usuarios de internet son el 92,8%. Si se analizan todos los datos presentados en la tabla 1, incluida en el estudio del INE, podrá comprobarse que la población estudiada son los menores de diez a quince años. Con una simple visión se puede percibir que los porcentajes aumentan progresivamente con la edad, llegando a rozar el 100% en las tres conductas analizadas en la última edad de la franja. Con este panorama de uso de dispositivos

y de conexión a internet, prácticamente es incuestionable decir que la formación en ciberseguridad debe estar en las escuelas.

Tabla 1. Menores usuarios de TIC

Menores usuarios de TIC en los tres últimos meses. Año 2020
Porcentajes de población de 10 a 15 años

	Usuarios de ordenador en los últimos tres meses	Usuarios de internet en los últimos tres meses	Disposición de móvil en los últimos tres meses
TOTAL	91,5	94,5	69,5
Por sexo			
Hombres	90,8	93,4	67,8
Mujeres	92,3	95,7	71,3
Por edad			
10 años	81,5	86,7	22,1
11 años	88,9	92,4	41,4
12 años	91,5	92,8	68,8
13 años	93,4	95,9	88,1
14 años	95,9	99,1	92,8
15 años	96,3	99,2	95,7

Fuente: Instituto Nacional de Estadística (2020, p.3)

Por otro lado, en el caso concreto de las redes sociales, "al no existir un adecuado tratamiento de la información, se expone a los menores de edad a diversos peligros, y por ende a la vulneración de derechos como el de la privacidad o intimidad" (Pineda y Jiménez, 2020, p.111). Fundamentalmente, el gran problema es que los niños y niñas están creando identidades digitales en diversas redes sociales en un momento en el que sus personalidades son altamente influenciables. Un estudio reciente, realizado por la empresa Qustodio (2020), evidencia que en España la red social más usada por menores de 15 años es Instagram. De hecho, 1 de cada 2 pequeños tiene cuenta en esta aplicación.

Tras añadir estos hechos a nivel nacional, los cuales representan el frente más técnico de la justificación, llega la hora de incluir sucesos reales que contrastan con las distintas explicaciones y estadísticas presentadas.

Para dar comienzo a las razones concretas que demuestran la necesidad de abordar cuestiones de ciberseguridad y de redes sociales con el alumnado, deben hacerse desde la evidencia de la problemática en el CEIP San Fernando de Santa Cruz de Tenerife en un aula de

sexto curso de primaria hace dos años. En aquel momento el autor del TFE formaba parte del claustro docente desde la posición de docente en prácticas, y lo cierto es que se tuvo la oportunidad de participar en unos talleres impartidos por la Consejería de Educación de Canarias.

En estas actividades se abordaron distintos riesgos y peligros existentes al acceder a internet y a las redes sociales. La ponente realizó una pregunta al gran grupo: "¿Cuántos de vosotros tenéis un smartphone y alguna red social?" Previamente al inicio de este taller, la misma empleada de la Consejería de Educación había comentado que el porcentaje de alumnos con móvil (en sexto de primaria) suele ser de un 80% y suelen tener 1 o 2 redes sociales, siendo Instagram y WhatsApp las más habituales. Sin embargo, en este caso levantó la mano la totalidad de la clase, teniendo la mayoría de ellos 3 o 4 redes. Evidentemente, esto causó una enorme preocupación en el tutor, el cual no tenía conocimiento de dicha situación, a pesar de estar ya situados en el segundo trimestre. Sin embargo, si se analiza de forma pautada y clara las respuestas de los niños y niñas, se verá que tienen mucho sentido, ya que la mayoría de los referentes o personajes públicos cuentan con varias redes sociales, las cuales patrocinan y referencian de forma continua en cada una de ellas.

Esto suele generar un efecto dominó en los registros en redes, ya que cada menor se ve obligado a tener presencia digital en todas ellas para poder contemplar toda la vida (costumbres, vestimentas, lugares preferidos, etc.) de sus ídolos. Por supuesto, también son empleadas para fines de contacto entre iguales y para compartir detalles y contenido multimedia. Justamente de esta manera, niños y niñas con 11 o 12 años comienzan a tener una identidad digital en decenas de páginas web.

Presentada esta primera razón, lo realmente preocupante llegaría en la segunda pregunta: "¿Cuántos de vosotros enseñáis a vuestras familias el teléfono para que haya un mínimo control?" Solamente levantó la mano una discente, la cual contestó que mostraba una vez por semana todo su historial y sus aplicaciones. Tras dicha respuesta, el resto del alumnado se burló de la pequeña con comentarios como: "Vaya pringada", "Ni de broma enseño mi móvil a mis padres", "Antes muerta…", "¡Sí hombre! Tiro el móvil por la ventana", "La niñita de papá y mamá", etc. Sin lugar a duda, esto ya generó un ambiente de tensión y de aire defensivo en el gran grupo, lo cual dificultaría, en gran medida, que la ponente pudiera mostrar pautas de ciberseguridad a los niños y niñas.

Desde esta tesitura, el planteamiento de enseñanza de las actitudes y contenidos en ciberseguridad debe ser lúdico y llamativo para el alumnado, ya que se ha visto de forma clara que, si se presenta de forma tradicional, pueden obtenerse actitudes defensivas y contrarias al aprendizaje. Además, se debe recordar que en esta franja de edad (entre 11 y 12 años) se da mucha relevancia a la privacidad, pues es el inicio de la adolescencia. Por este motivo, es clave adentrar todo este aprendizaje, el cual puede llegar a parecer intrusivo, desde una perspectiva más dinámica y divertida. Es justo en este punto en el que entra la gamificación. El planteamiento de la programación se basa en partir desde las áreas del currículum, pero incluyendo elementos de ciberseguridad y redes sociales, trabajando todo de forma orgánica alrededor de una narrativa y un contexto gamificado llamativo, el cual actuará como "un juego de luces y sombras" que camuflará las intenciones del docente. Con esto, se pretende evitar lo que le ocurrió a la ponente de los talleres, la cual presentó sus intenciones con demasiada velocidad a los menores. En otras palabras, se debe generar una misma frecuencia de onda con el alumnado, con el objetivo de que las señales que se envíen lleguen con menor esfuerzo y generen un aprendizaje actitudinal efectivo.

Tras describir esto y conociendo las implicaciones, surge la gran cuestión que motiva la creación de este diseño: ¿Cómo pueden cambiarse las conductas y hábitos en la red de los menores de edad? Desde este interrogante se iniciará el planteamiento de las metas o fines de la posible solución que representa este proyecto de innovación.

1.2. Objetivos del TFE

1.2.1. Objetivo general

- Diseñar una propuesta de gamificación como medio de aprendizajes de conductas seguras en la red.

1.2.2. Objetivos específicos

- Determinar los patrones visibles en ciertas tipologías de ciberacoso.
- Estructurar un aprendizaje lúdico del funcionamiento óptimo de las redes sociales.
- Relacionar elementos avanzados de la competencia digital dentro del marco curricular.
- Evaluar el diseño propuesto empleando la experiencia de profesionales del sector educativo y del área de la ciberdelincuencia.

2. Marco teórico

2.1. Gamificación

Si se buscan las distintas metodologías emergentes educativas relacionadas con los juegos, videojuegos y otras experiencias lúdicas, es altamente probable que se encuentre un enfoque que no para de ganar miles de adeptos. Este no es otro que el representado con el vocablo "gamificación". Curiosamente, cuando se trata de localizar representaciones conceptuales y procedimentales de esta metodología, puede verse que está relacionada, en mayor medida, a múltiples esferas del mundo económico. De hecho, se puede comprobar que está más ligada a este plano empresarial que al educativo, lo cual tiene que ver principalmente con su nexo existente con la productividad de los trabajadores y trabajadoras.

En otra instancia, tomando distancia de este debate, aún no se ha explorado el concepto definitorio de gamificación. Cabe decir que existen varias interpretaciones del significado de esta palabra en función de los autores o investigadores que lo aborden. Por ello, se tomarán dos planteamientos distintos de dicha definición, con el objetivo de hacer un análisis más amplio y rico. Para empezar, Werbach y Hunter (2012) aseguran que "la gamificación es el proceso de manipulación de la diversión para servir objetivos del mundo real" (p.6). Mientras que Teixes (2015) afirma que "la gamificación es la aplicación de recursos propios de los juegos (diseño, dinámicas, elementos, etc.) en contextos no lúdicos, con el fin de modificar los comportamientos de los individuos, actuando sobre su motivación, para la consecución de objetivos concretos" (p.18). Con una mínima lectura reflexiva se comprende que los autores visualizan este enfoque metodológico como una forma de lograr objetivos por medio de un engaño. La cuestión es la siguiente: ¿A quién se engaña y cómo se hace?

2.1.1. Tipos de jugadores

Al entrar a responder este interrogante, lo primero que debe abordarse son los individuos que vamos a manipular de forma positiva con la gamificación. Evidentemente, una parte importante de todo proyecto son las personas que participan y se ven inmersas en él, ya que cada una presenta un perfil distinto con motivaciones distintas. Si se analizan bien las características propias de cada participante de la experiencia gamificada, se podrá dar mejor respuesta a sus necesidades, logrando aumentar su productividad en el proceso de enseñanza-aprendizaje.

Prácticamente todos los sectores que emplean la gamificación siguen la taxonomía de tipos de jugadores, presentada por el profesor Richard Bartle (diseñador de videojuegos y profesor de universidad en Essex). Es más, la extensión de esta clasificación ha trascendido a prácticamente todos los documentos académicos existentes sobre este eje del marco teórico. Por este mismo motivo, se mencionarán los tipos presentados por Bartle (2008):

- "Killer" (Asesino). Estos jugadores necesitan momentos de competitividad con otros iguales. Para ellos los momentos de enfrentamiento o competición son lo más importante en una experiencia de juego. Este perfil requiere de espacios y momentos en los que expresar sus victorias socialmente.
- "Achiever" (Caza-logros). Disfrutan al alcanzar los objetivos planteados en el juego. Disfrutan extremadamente de sistemas de recompensas o de medallas, los cuales denoten su buen desempeño en su trabajo. Sus necesidades no suelen incluir la victoria, sino sentirse cómodos con las tareas y recursos de trabajo.
- "Socialiser" (Socializador). Necesitan interactuar con otros jugadores para poder seguir avanzando en la gamificación. Además, la motivación y la atención depende mucho de que se incluyan múltiples momentos de trabajo cooperativo o colaborativo, permitiendo interacciones sociales continuas.
- "Explorer" (Explorador). El último tipo presentado representa a personalidades que se diviertan al descubrir nuevas zonas y detalles del campo o mundo fantástico. Secretos o lugares ocultos, puzles en el entorno jugable, historias o leyendas de personajes creados. Todos estos aspectos motivan a esta tipología de jugador.

Es importante comentar que han existido ciertas revisiones a esta lista de cuatro modelos, logrando una de ellas presentar una de ellas una nueva esquemática de usuarios no contemplados previamente. Concretamente, Marczewski (2015) presenta una clasificación hexagonal, la cual ya tiene presente los tipos ya comentados, tal y como puede verse en la figura 1. No obstante, añade dos nuevos:

- "Philanthropist" (Filántropo). Su único deseo es avanzar ayudando al resto de los jugadores a cumplir los distintos objetivos y situaciones presentes en la gamificación.
- "Disruptor" (Alterador). Su principal objetivo es cambiar el sistema gamificado, ya sea para bien o para mal. Su atención depende plenamente de los imprevistos que sea capaz de provocar.

Figura 1. Hexágono con los tipos de jugadores. (Marczewski, 2016)

2.1.2. Diseño de una gamificación I: modelo de creación

Tras haber abordado de forma clara el público posible que puede encontrarse en una gamificación, sin embargo, todavía no se ha respondido al cómo diseñar el engaño o manipulación de la que se hablaba inicialmente. Por suerte, Teixes (2015) presenta un modelo con los pasos a seguir en el diseño de un entorno gamificado:

1- Definir los objetivos del sistema. Los objetivos tienen que poder cambiar la problemática que se quiere solucionar, especialmente si se trata de comportamientos o pautas mentales de las personas. Estos son mucho más complicados de cambiar.

2- Comprender la audiencia objetivo y el contexto. Lógicamente no es lo mismo abordar el ámbito empresarial con adultos que el ámbito educativo con menores. Por otro lado, deben analizarse condiciones como el lugar, contexto socioeconómico, nivel cultural, entre otros.

3- Definir las conductas objetivo. En este momento deben diseñarse las actividades y tareas que saquen a la luz los comportamientos deseados, los cuales sustituyen los problemáticos de una forma lúdica. Pero aún falta lo más importante, el espejismo que permite que esto se haga sin que el público se dé cuenta.

4- Construir el sistema gamificado. En este punto se comienza a desarrollar todas las componentes de la gamificación, es decir, todos los elementos del engaño (mecánicas, dinámicas y estética).

5- Implementar. Puesta en práctica de todo lo diseñado.

6- Mantener la integración actualizada. En función de lo que se haya observado en la aplicación se tendrán que optimizar todos los elementos que puedan mostrar fallas. De esta forma, siempre se tendrá garantizada la atención de los asistentes.

2.1.3. Diseño de una gamificación II: mecánicas, dinámicas y estéticas

Luego de explorar el método de diseño al completo de una programación basada en gamificación, es primordial ahondar en su cuarto punto, el cual versa sobre la construcción de los elementos principales de la metodología. Estos componentes son comúnmente agrupados en un marco de referencia denominado como MDA (Mechanics, Dynamics, Aesthetics). De hecho, investigadores educativos han afirmado que "The MDA framework is a postmortem analysis of the elements of a game. It helps us use systems-thinking to describe the interplay of those game elements and apply them outside of games" [El marco de referencia MDA es un análisis post mortem de los elementos de un juego. Este ayuda a usar sistemas de pensamiento que describen la interacción entre dichos elementos de juego y su uso en contextos externos a los juegos] (Zichermann y Cunningham, 2012, p.35). Dicho esto, es momento de desglosar cada una de las letras que componen esta sigla:

- "Mechanics" (Mecánicas). Una definición aceptada es la que define a las mecánicas "como principios, reglas o mecanismos que gobiernan el comportamiento a través de un sistema de incentivos, feedback y recompensas con un resultado razonablemente predecible" (Herranz y Colomo-Palacios, 2012, p.41). En otras palabras, son aspectos provenientes de los juegos que motivan al jugador a avanzar en la gamificación continuamente. Es importante comentar que estos puntos deben atender a los perfiles de usuario que se plantearon en el apartado anterior, ya que cada participante tiene sus propios potenciadores de motivación. No obstante, la selección puede hacerse desde una taxonomía general, como por ejemplo la que presenta Oliva (2016):
  - ❖ Puntaje. Método cuantificable y registrable de la gamificación. Suelen emplearse puntos o medallas con ciertas graduaciones.
  - ❖ Niveles. Sistema evolutivo análogo a una escalera de aprendizaje. Superar un peldaño implica la obtención de ciertos conocimientos.
  - ❖ Posesiones virtuales. Objetos imaginarios que son registrados como pertenencia.
  - ❖ Clasificaciones. Tablas o rankings que indican el posicionamiento de los participantes.

- ❖ Desafíos. Situaciones complejas que deben superarse con una o más competencias.
- ❖ Premios o retribuciones. Trofeos que aportan satisfacción ante el cumplimiento de ciertos objetivos o metas.

- "Dynamics" (Dinámicas). Teixes (2015) propone que las dinámicas son elementos de control que pueden estar presentes en los juegos, sin embargo, no son originarios de los mismos. Sería preciso decir que si las mecánicas son los mecanismos que fomentan la motivación, las dinámicas vendrían a ser los sistemas de seguridad que garantizan su correcto desempeño. El mismo autor defiende la existencia de las siguientes:
  - ❖ Recompensas. Premios físicos o virtuales que pretenden funcionar como un refuerzo positivo de una conducta deseada.
  - ❖ Estatus. Concepción social basada en el reconocimiento propio y de otros jugadores. Tiene una relación clave con las mecánicas de puntaje, niveles, clasificaciones…
  - ❖ Logros. Recompensa irreal que se activa al completar algún objetivo, ya sea individual o grupal. Suelen tener una graduación de dificultad, de tal manera que nunca lleguen a ser frustrantes para ciertos participantes.
  - ❖ Autoexpresión. Es importante dar márgenes de creatividad a los usuarios a la hora de actuar o de generar producciones personales. También es conveniente incluir elementos como personalización de personajes, avatares, ítems imaginados…
  - ❖ Competición. La competitividad es una forma muy efectiva de garantizar que los jugadores avancen motivados a la meta, especialmente en los que se ajustan al perfil asesino. No obstante, siempre hay que tener ciertos límites que eviten momentos desastrosos, los cuales pueden ir desde episodios incómodos a casos de violencia verbal o física.
  - ❖ Altruismo. Esta dimensión siempre crea un clima positivo de juego, ya que todas las interacciones que busquen ayudar, sin recibir nada a cambio, suelen terminar generando sentimientos de deuda muy beneficiosos.
  - ❖ Feedback. Este aspecto es básico en cualquier esfera del proceso de enseñanza-aprendizaje. Por ello, cobra una mayor relevancia en una metodología que se basa en crear ilusiones lúdicas y atractivas para el avance del alumnado. Es primordial que cada integrante conozca su el estado de su progreso en todo momento.

- ❖ Diversión. El apartado lúdico es vital para que todo lo demás funcione. No existirá posibilidad de manipular y alterar el problema si no se hace con el público distraído.

- "Aesthetics" (Estéticas). Según Hunicke, Leblanc y Zubek (2004), las estéticas hacen referencia a las emociones que deseamos provocar en los jugadores al interactuar con el sistema de juego. Estos mismos autores presentan un catálogo de ocho posibilidades emocionales:
  - ❖ "Sensation" (Sensación). Disfrute libre en la experiencia.
  - ❖ "Fantasy" (Fantasía). Sentimiento estupor fantasioso.
  - ❖ "Narrative" (Narrativa). Historia que atrape al jugador.
  - ❖ "Challenge" (Reto). Presencia de situaciones obstaculizadoras.
  - ❖ "Fellowship" (Compañerismo). Avance a través la cooperación.
  - ❖ "Discovery" (Descubrimiento). Mapeado inexplorado que recorrer.
  - ❖ "Expression" (Expresión). Sistema que lleve a momentos de introspección.
  - ❖ "Submission" (Sumisión). Juego como pasatiempo.

2.1.4. Diseño de una gamificación III: conexión con otras metodologías emergentes

Torres-Toukoumidis y Romero-Rodríguez (2018) manifiestan que:

> La gamificación en el aula puede (. . .) ser implantada transversalmente en metodologías como el aula invertida (flipped classroom), el Aprendizaje Basado en Proyectos o el Aprendizaje Basado en Problemas o en modalidad de educación presencial, semi-presencial (blended) o virtual (e-learning) (p.64).

En otras palabras, este enfoque lúdico tiene una magnífica compatibilidad con otros sistemas metodológicos innovadores, los cuales suelen tener como premisa principal el protagonismo del discente.

Partiendo de esta idea, es primordial introducir al Aprendizaje Basado en Problemas (ABP) como el punto de partida programático de la gamificación "Exploit City. Según Arpí et al. (2012), el ABP es una metodología que promueve la iniciativa del discente, trabajar cooperativamente y dando una autonomía (siempre con unos momentos de guía) hasta la finalización de un proyecto. Puede partirse desde un interrogante, que es exactamente el caso de esta propuesta: "¿cómo pueden cambiarse las conductas y hábitos en la red de los menores

de edad?". Obviamente, esta cuestión puede resolverse desde la práctica en el aula, unificando los contenidos teóricos con demostraciones y simulaciones de la realidad. Es más, esta metodología genera oportunidades de aprendizaje en las que el alumnado toma completamente el protagonismo.

Visto esto, no debe malinterpretarse esta última idea, ya que el docente sigue teniendo funciones claves, "puesto que los grupos de ABP dependen en gran medida de las habilidades de los profesores tutores para fomentar la participación del estudiante, el trabajo en equipo y el pensamiento de orden superior" (Arpí et al., 2012, p.15). Efectivamente, todos los cambios didácticos innovadores en la enseñanza están abogando por un enfoque de trabajo en cooperación del alumnado, y es justo aquí donde entra en juego el estilo pedagógico de aprendizaje que busca una socialización y desarrollo interpersonal, permitiendo el andamiaje entre grupos de iguales. Este no es otro que el aprendizaje cooperativo.

Negro y Torrego (2014) introducen que "los proyectos cooperativos son una excelente oportunidad para construir el currículo . . . porque implican situaciones contextualizadas de aprendizaje, problemas y temas" (p. 185). Este razonamiento es lógico y sensato a la hora de abordar un problema, ya que un grupo de personas puede llegar antes a una solución que un individuo por separado. No obstante, es mucho más efectivo si dentro de dicha agrupación se establecen roles y funciones diferenciadas, las cuales se complementan para dar mejor forma a la respuesta al dilema o punto de partida (tarea o actividad). "Ser un grupo estructurado (con roles) con unos objetivos claros, conocidos y compartidos por todos, con los que se identifican todos los componentes del grupo" (Domingo, 2008, p.235).

Desde esta combinatoria metodológica, y teniendo como epicentro a la gamificación, se da respuesta completa al apartado de diseño. De esta manera, la estrategia lúdica queda envuelta por los otros métodos pedagógicos pertinentes. Sin embargo, existe una última esfera que no se ha abordado en amplitud. Si el educando es el protagonista de este sistema, ¿cuál es el motivo de plantear la gamificación como una manipulación o alteración?

2.1.5. La última frontera de la gamificación: aceptación voluntaria del fraude

Tras haber contestado el interrogante que se plantea al inicio (mostrando cómo diseñar una gamificación), lo cierto es que todavía queda un detalle relevante que indicar. A pesar de que el objetivo de toda gamificación es implantar unos conocimientos actitudinales y

procedimentales, que solucionen un problema determinado de forma clandestina, al final es necesario que el alumnado quiera adquirir los conocimientos. No se puede olvidar que la enseñanza es una relación bilateral en la que siempre tiene la dominancia el discente. En otras palabras, un educando debe estar dispuesto a adquirir las ideas que un docente quiere alterar o ampliar con su programación. Esto no es diferente en el caso de una propuesta gamificada. Ripoll (2016) también aborda esta misma idea en su investigación en la esfera universitaria:

> Por otra parte, el reto es conseguir que el alumno perciba que decide cada una de las acciones que se le proponen y que las lleva a cabo por voluntad propia. Esta definición es la misma que aplicaríamos a un juego. Dicho de otra forma, debemos conseguir que los alumnos jueguen con los contenidos que proponemos, viviéndolos como retos que quieren superar (p.26).

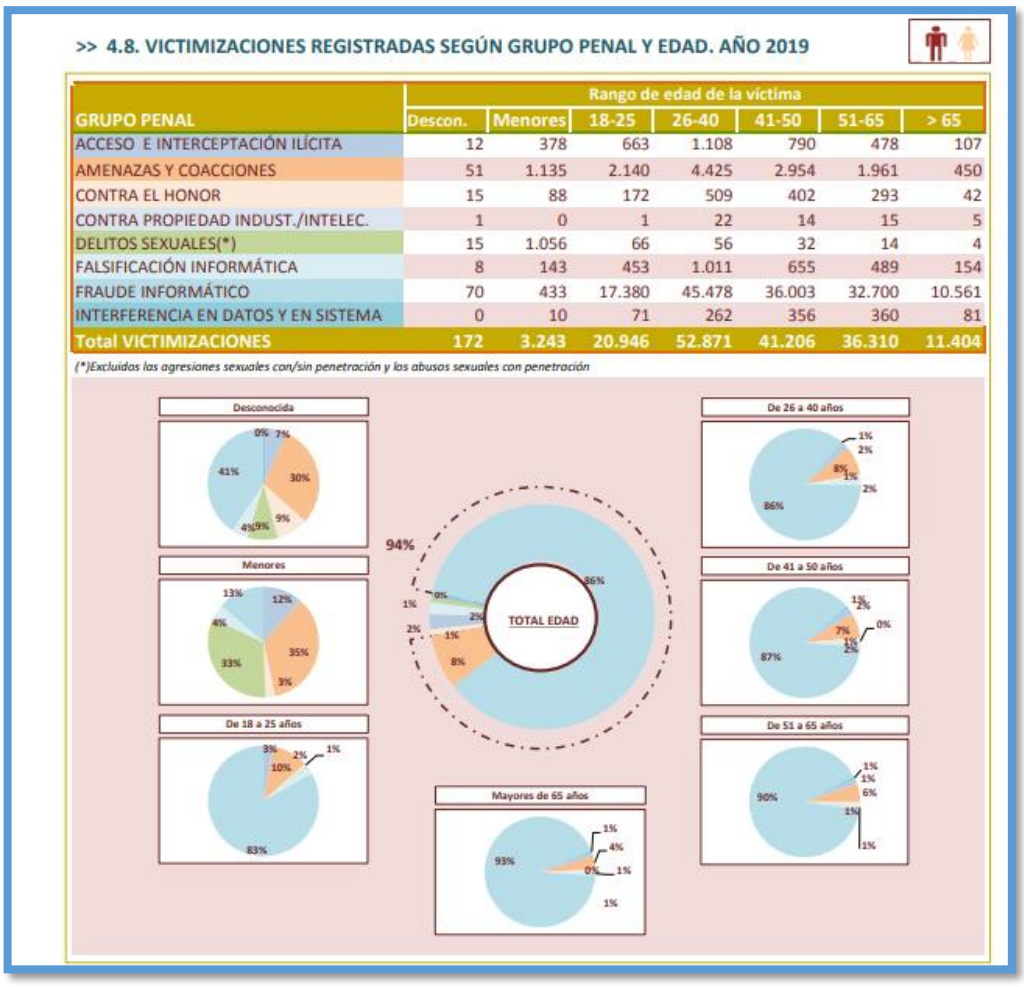
La realidad de todo este proceso metodológico se traduce en que, si la gamificación atiende correctamente a las necesidades y perfiles de su público, es altamente probable que llegue a ser exitosa. Por supuesto, también debe tenerse en cuenta la complejidad de los contenidos curriculares y de la temática a trabajar, ya que, en función de su nivel de abstracción, el maestro o maestra tendrá que ultimar mejor los detalles programáticos (criterios, metodologías, secuenciación, temporalización, actividades, evaluación…). Justo en esta delgada línea se sitúa este proyecto, el cual aborda dos realidades virtuales que también forman parte del marco teórico. Estas son la ciberseguridad y las redes sociales.

2.2. Ciberseguridad

Los niños y niñas nacidos en el siglo XXI cuentan con múltiples recursos tecnológicos con conexión a una red con infinitos contenidos de todo tipo de ramas del conocimiento y entretenimiento. Ante este hecho, muchas personas podrían pensar que es completamente habitual y lógico que esto pase, y en cierto sentido, tienen razón. Emplear un dispositivo tecnológico en edades tempranas no tiene por qué ser malo, siempre y cuando exista una formación útil y efectiva sobre los riesgos y procesos involucrados en su uso. Por desgracia, la mayoría de los cursos y talleres que tratan de aportar conductas seguras y usos responsables de la tecnología e internet no están teniendo un gran impacto, lo cual queda patentado con datos como los aportados por el siguiente estudio del Ministerio de Interior (2019): la cibercriminalidad ha pasado de un 4,6% sobre el total de todas las infracciones penales en el

año 2016 a 9,9% en 2019 (siendo el 79,6% de los detenidos de nacionalidad española), el total de víctimas registradas en las denuncias asciende a 166152 personas en 2019 (un 38% más que en 2018) y las denuncias de ciberdelincuencia con víctimas menores de edad en 2019 son 3243 (1185 son niños y 2058 son niñas). Analizando este último dato, es importante destacar la tipología de los delitos, por eso se adjunta la tabla 2, presentada por esta investigación gubernamental. En ella podrá observarse de forma clara que los delitos de amenazas y coacciones (relacionados con el ciberacoso) y de carácter sexual tienen unos porcentajes realmente alarmantes en el grupo de los menores. Por otro lado, hay que recordar que muchos de estos delitos ni siquiera llegan a denunciarse por la incapacidad de demostrar las actitudes delictivas o por miedo, dando lugar a la famosa cifra negra de crímenes de ciberdelincuencia sin denuncia. Pero es que, si se observan los casos denunciados, podrá visualizarse que solamente el 15,1% de las situaciones logran esclarecerse por completo.

Tabla 2. Victimizaciones registradas según grupo penal y edad



>> 4.8. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	12	378	663	1.108	790	478	107
AMENAZAS Y COACCIONES	51	1.135	2.140	4.425	2.954	1.961	450
CONTRA EL HONOR	15	88	172	509	402	293	42
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	1	22	14	15	5
DELITOS SEXUALES(*)	15	1.056	66	56	32	14	4
FALSIFICACIÓN INFORMÁTICA	8	143	453	1.011	655	489	154
FRAUDE INFORMÁTICO	70	433	17.380	45.478	36.003	32.700	10.561
INTERFERENCIA EN DATOS Y EN SISTEMA	0	10	71	262	356	360	81
Total VICTIMIZACIONES	172	3.243	20.946	52.871	41.206	36.310	11.404

(*)Excluidas las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

Fuente: Ministerio de Interior (2019, p.40)

En este contexto, se hace más que patente la necesidad de incluir en el sistema educativo informaciones amplias sobre conductas y procedimientos de seguridad en la red. Esto es a lo que, comúnmente, se llama ciberseguridad. De hecho, la mayoría de los autores como, por ejemplo, Giant (2016) la definen así:

> La ciberseguridad se refiera al uso seguro y responsable de los productos de la tecnología de la información y comunicación (TIC), incluyendo Internet, los dispositivos móviles y de comunicación y los instrumentos tecnológicos diseñador para guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales, etc. (p.16)

Sin embargo, más allá de las denuncias y los delitos penales recogidos en el Código Penal, ¿existe alguna base legal en educación que obligue a actuar ante esta terrible realidad? Pues la respuesta no es otra que sí, es más, existe absoluta necesidad de actuar por obra de uno de los derechos fundamentales de la Constitución, y no es otro que el derecho a la educación (artículo 27).

2.2.1. Artículo 27.2 de la Constitución en ciber-amenaza

"La educación tendrá por objeto el pleno desarrollo de la personalidad humana en el respeto a los principios democráticos de convivencia y a los derechos y libertades fundamentales" (art. 27.2 CE). Este subpunto es, posiblemente, el más importante dentro del artículo 27 de la Constitución Española, ya que es el que más carga legal conlleva en cuento a la educación del menor. Si se hace un análisis minucioso de la oración, podrá verse que su principal premisa es la de cooperar en la creación de una personalidad propia y única para cada discente, siguiendo los valores y libertades propios de una democracia. No obstante, hay un enorme problema en todo esto, y es que la psique del menor obtiene aprendizajes de múltiples influencias, no solamente las ligadas a la escuela. Hablamos de múltiples tipos de influjos: escolar, familiar, amistades, medios de comunicación y, por supuesto, los recursos tecnológicos e informáticos. Todos ellos causan enormes alteraciones y contradicciones en la mente humana, sin embargo, está claro que uno de ellos ha ganado un papel mucho más relevante en las últimas décadas, y no es otro que el relacionado a la red y las tecnologías.

Si se ahonda más en esta teoría, lo cierto es que todos los aspectos que involucran el uso de internet en edades tempranas llevan ligado un avance de conocimiento que, normalmente,

se adquiere en etapas superiores. En muchas ocasiones, ciertas ideas pueden llegar a superar lo que un niño o niña puede llegar a procesar en su etapa de pensamiento. Por ejemplo, si un discente descubre (accidentalmente) términos relacionados con la sexualidad en algún buscador en edades entre los seis u ocho años, seguramente no tenga la capacidad de gestionarlo mentalmente de una forma óptima. Este tipo de situaciones, independientemente de las ideas y concepciones ideológicas que se vean implicadas, pueden llevar a alteraciones de la personalidad y a efectos madurativos inesperados. Esto afectará negativamente al proceso educativo sin lugar a duda.

Una vez explicado esto, se deja el terreno preparado para abordar los efectos de la red que pueden provocar estos momentos incómodos para la personalidad del alumno o alumna. Concretamente, se dividen en dos tipologías: software malicioso o "malware" y contenidos inadecuados.

2.2.2. Peligros en la red I: software malicioso

Para empezar, se plantearán los distintos métodos invasivos y malignos que pueden afectar a los dispositivos de los menores. En su mayoría, estos programas pretenden extraer y robar información personal de sus víctimas, aunque también pueden existir fines meramente caóticos y destructivos. Cepeda (2019) plantea una taxonomía clara de los más comunes, la cual se desarrollará por medio de explicaciones propias y de múltiples expertos en materia de ciberseguridad. Por este motivo, se ha diseñado la tabla 3 en conexión con esta clasificación.

Tabla 3. Tipos de software malicioso

Software malicioso	Explicación de su procedimiento
Troyano	Ficarra (2002) aporta la siguiente idea: "Son los más peligrosos desde el punto de vista de la seguridad, porque una vez instalado el virus en la computadora, los teleoperadores del sistema denominados crackers son capaces de manejarla a distancia" (p.66). Este software maligno suele estar oculto en archivos con extensiones habituales, haciéndose pasar por algún contenido sano.

Gusano	Bermúdez (2005) dice que "en informática, un gusano es un virus o programa que no altera los archivos, sino que reside en la memoria y se replica a sí mismo" (p.6). El objetivo de este programa malicioso es ralentizar o congelar el funcionamiento del dispositivo.
Spam	Concretamente, esta palabra representa la bandeja del correo electrónico en la que se reciben e-mails con contenidos no deseados de todo tipo. Muchos virus vienen adjuntos en este tipo de mensajes.
Spyware	Según Egele et al. (2007), el término "spyware" hace referencia a un código maligno que se instala clandestinamente en los ordenadores de ciertos usuarios. Poco a poco, ese programa capta toda la información del usuario (cuentas con contraseñas, hábitos, búsquedas, etc.). Suele ir contenido en algún archivo, pero a diferencia del troyano, este actúa sin dar ningún aviso de su existencia, y tampoco pretende dañar al dispositivo que lo contenga.
Keylogger	Este software registra todas las pulsaciones que se realizan en el teclado, enviándolas posteriormente al ordenador del invasor. Como es lógico pensar, lo más probable es que se extraigan datos personales de todo tipo con esta mecánica.
Phishing	Según Jakobsson (2005), un ataque común de "phishing" se basa en la obtención de los datos de inicio o autentificación de un usuario por medio de una interfaz o red mensajes engañosa (web clonada, e-mail, SMS falso, etc.). Este recurso suele emplearse especialmente para robar datos de acceso a todo tipo de cuentas, especialmente bancarias.
Pharming	Este es una evolución del "phishing", ya que cuando se busca un sitio web determinado se establece un nuevo recorrido a un punto de la red falso por alguna variación en los datos de navegación. Conforme a Brody, Mulig y Kimball (2007), los "pharmers" elaboran una gran red en la que atrapar a usuarios, lo cual logran envenenando los servidores de Sistema de

	Nombres de Dominio (DNS). De esta forma, el sistema DNS reconoce a ciertas direcciones web como seguras (a pesar de no serlo).
Rogue	Software camuflado como antivirus que manda avisos constantes de que existen amenazas o programas maliciosos (no son reales). Una vez se activa para eliminar esos supuestos virus, instala programas malignos.
Bots y Botnets	Este ataque se basa en captar ordenadores de usuarios con distintos recursos malignos (especialmente con e-mails en spam) para luego controlarlos por completo. De esa forma el dispositivo se convierte en un "bot", pasando a formar parte de toda una red llamada "botnet". El ciberdelincuente luego podrá usarla para múltiples fines delictivos.
Ransomware	"Ransomware is a category of malicious sofware which, when run, disables the functionality of a computer in some way" ["Ransomware" es una categoría de software malicioso que, cuando se ejecuta, deshabilita la funcionalidad de un ordenador de alguna manera] (O´Gorman y Mcdonald, 2012, p.2). Por ejemplo, cuando se abre una ventana emergente, la cual no puede cerrarse, bloqueando la pantalla.
Hoax	Este agrupa todos los bulos, cadenas de mensajes alterados y noticias falsas que se difunden por la red. Han cobrado mucha relevancia en los últimos años, especialmente por el auge de las redes sociales.

Fuente: Elaboración propia

2.2.3. Peligros en la red II: contenidos inadecuados para la integridad del menor

Entrando en el otro sector de peligros que pueden afrontar los pequeños y pequeñas en la red, es momento de comentar los que tienen que ver con las búsquedas en la red, es decir, todos aquellos contenidos no deseables que pueden crear conflictos y dilemas en la personalidad (especialmente en el lado emocional). Cepeda (2019) también se adentra en los distintos temas que deben evitarse a toda costa, presentando otra clasificación de gran extensión. Dicha lista de tópicos será la base para desarrollar la tabla 4.

Tabla 4. Tipos de contenidos inadecuados

Contenido inadecuado	Explicación
Pornografía	Un contenido al cual puede llegarse a través de miles de términos, y encima de manera no deseada. Es recomendable poner controles en los servicios de red para evitar sus entradas.
Pornografía infantil	En España es ilegal acceder a este tipo de multimedia, sin embargo, en ciertos puntos de la red como la "Deep web" o la "Dark web" puede hacerse. No obstante, dada a la complejidad de acceder a este punto de internet (navegadores especiales), esto no suele ocurrir.
Gore y snuff	Hace referencia a páginas con contenido sangriento y violento con un gran nivel de explicitud. Al igual que la anterior, son más comunes en zonas poco accesibles de la red, pero sí pueden encontrarse con navegadores normales en algunos casos.
Páginas con tendencias peligrosas y/o discriminatorias	Un ejemplo claro de estas páginas sería "La belleza azul", una moda en la que se contactaba con una cuenta anónima que ponía retos peligrosos y, en ocasiones, suicidas.
Ask.fm	Esta web funciona como una red social en la que una persona recibe preguntas y mensajes de forma anónima. Ha estado íntimamente relacionada a casos de ciberacoso.
Robo de información, envío de SMS, etc.	Existen múltiples servicios de suscripción con envíos de SMS, empleos sin permiso de datos personales, pagos mensuales con tarjeta…Todos ellos pretenden engañar a mentes altamente manipulables, especialmente las de menores aún en desarrollo.

Vídeos con contenido violento o agresivo	Al igual que con las páginas "Gore y snuff", también existen contenidos multimedia con este tópico como elemento central. En muchos casos, pueden encontrarse en lugares muy transitados en la red, especialmente en redes sociales.
Páginas con malware	Como es evidente, existen múltiples páginas como parte de sistemas de entramado "phishing" o "pharming", las cuales son un riesgo probable para cualquier persona. Por tanto, también para niños y niñas.
Juegos con violencia gráfica excesiva online	Videojuegos que causan emociones estresantes y desadaptativas a los menores a causa de su carácter violento y bélico.
Contenido inimaginable	Dentro de este punto es especialmente importante nombrar las zonas más peligrosas de internet. Estas son la "Dark web" y la "Deep web". En estos puntos de la red existen contenidos relacionados con cientos de delitos. De hecho, acceder a ellas ya es un crimen. Los menores no se encuentran a salvo de ellas por su gran curiosidad, lo cual puede llevarlos a descubrir los métodos de acceso a las mismas.

Fuente: Elaboración propia

2.2.4. Ciberseguridad en conexión con las redes sociales

Tras haber dejado atrás todas las amenazas que justifican la necesidad de formar en ciberseguridad a los menores, es clave decir que existe un punto mucho más crítico que los que se han tratado anteriormente. De hecho, se han omitido deliberadamente detalles de enorme gravedad para los menores, ya que tienen que ver con una esfera que tendrá su propio marco de contenidos dentro del proyecto. Este eje no es otro que el de las redes sociales. Es imposible entender todo el avance de la ciberdelincuencia sin hablar de ellas, ya

que muchos de estos virus y dilemas han surgido por su alta masificación. Avogadro (2009) lo deja claro con la siguiente afirmación:

> Las redes sociales abren el espectro a una gran cantidad de circunstancias, como siempre en la cibercultura, de polaridades. Por una parte, acercan a personas con intereses comunes y por otra, es la puerta de entrada para que se cometan delitos. (p.1)

Después de haber aportado esta explicación, es el momento de comenzar la inmersión en esta nueva realidad intangible, la cual invade todas las vidas humanas hasta el punto de convertirlas en rutinas programadas y codificadas, las cuales son propias de la ciudad presentada por la película "The Matrix" (Wachowski, 1999).

2.3. Redes sociales

Esta línea teórica está altamente implicada con la anterior, sin embargo, esta merece tener su propio espacio reservado. Es innegable que el porcentaje de habitantes del mundo que accede a internet nunca deja de aumentar, pero mucho más evidente resulta decir que una de las razones principales de dicho aumento son las redes sociales. No obstante, ¿cómo se define algo tan amplio y variable como una red social? Orihuela (2008) aporta la siguiente descripción: "las redes sociales en línea, como LinkedIn, Facebook o Tuenti, son servicios basados en la web que permiten a sus usuarios relacionarse, compartir información, coordinar acciones y en general, mantenerse en contacto" (p.58). Si se hace un análisis certero de esas palabras, se podrá comprobar que nombra dos portales con fines muy distintos. Estos son LinkedIn (red especializada para el empleo) y Facebook (red diseñada para, los cuales siguen vigentes en la actualidad con millones de usuarios en activo. Múltiples autores se esfuerzan mucho en distribuir las redes en base a ciertos criterios y aspectos subjetivos, lo cual vuelve altamente complejo decantarse por una organización determinada. A pesar de ello, se ha decidido tener en cuenta la taxonomía presentada por el autor Leiva-Aguilera (2009), el cual tiene en cuenta tres puntos clave para distribuir las redes sociales: "especialización (horizontal y vertical), ámbito vital (personales y profesionales) y un grupo final donde cabe una mezcla de todo lo anterior (híbridas)" (p.16).

2.3.1. Tipos de redes sociales

Retomando la taxonomía presentada en el punto anterior, se abordarán cada una de las distintas posibilidades de plataforma social que podemos encontrar en internet.

- Redes sociales de especialización. Esta tipología es establecida en base a los tópicos o categorías temáticas que se alojan en dicha red.
  - ❖ Redes sociales horizontales. Pueden abordarse todo tipo de conversaciones y divulgarse miles de informaciones y contenidos de múltiples áreas de interés. Solamente quedan fuera o sujetas a denuncia las ideas que vulneren las políticas y normativas legales. Un ejemplo es Twitter.
  - ❖ Redes sociales verticales. Se diseñan con un tópico central concreto (fotografía, viajes, cocina, etc.) en mente. El objetivo es reunir a usuarios con dicho interés, generando una comunidad especializada. Un ejemplo es Flickr.
- Redes sociales de ámbito vital.
  - ❖ Redes sociales personales. Se priorizan los usos personales. Es decir, se establecen contactos y conversaciones con el objetivo de hacer amigos, mantener el contacto, vivir momentos de ocio… Un ejemplo de este tipo es Facebook.
  - ❖ Redes sociales profesionales. Se diseñan con el fin de mejorar la red de contactos laborales y obtener una gama más amplia de ofertas de empleo. Un ejemplo claro es LinkedIn.
- Redes sociales híbridas. Este tipo de redes se diseñaron en alguna de las otras tipologías, pero han ido ganando otros usos por meras iniciativas sociales. Ejemplos evidentes pueden ser los grupos de trabajo en Facebook o los canales dedicados a mejorar habilidades de búsqueda de empleo en TikTok.

A pesar de los usos que puedan tener en mente los programadores y diseñadores de las redes sociales, no puede olvidarse que, al incluir amplias bases de usuarios, los cuales no dejan de ser personas que componen la sociedad, seguramente estas puedan generar cientos de usos e iniciativas que no estaban pensadas en un principio. Por desgracia, muchas de estas nuevas alternativas de utilización no buscan fines positivos ni altruistas, sino que están relacionados con extender delitos del mundo físico al universo virtual (no olvidemos que la red no tiene fronteras). Desde esta perspectiva, los menores que entran en estas aplicaciones están

indefensos ante estas nuevas formas de atacar y dañar en la red, que no son otra cosa que métodos de ciberacoso.

2.3.2. Peligros en la red III: el ciberacoso en redes sociales

2.3.2.1. Ciberbullying

"El ciberbullying consiste en utilizar las TIC, principalmente internet y el móvil, para ejercer acoso entre iguales" (Garaigordobil, 2015, p.1069). Las informaciones o mensajes que suelen existir entre los menores suelen tener frases dañinas o difamatorias, las cuales suelen ser tremendamente efectivas y dolorosas en esas franjas de edad. Es primordial recordar que en esas edades la dignidad y el honor son más difíciles de mantener por no tener una mente y personalidad plenamente desarrolladas (retomando lo comentado con respecto al artículo 27.2 de la Constitución Española). Por otro lado, es importante destacar que en este delito de acoso no se incluyen mensajes con contenidos sexuales, ya que estos se encuentran tipificados en otros tipos de ciberacoso. Para dejar evidenciadas las características principales del ciberbullying, se presentarán a partir de unos puntos de elaboración propia.

- Relación. Acosador y víctima son de edades similares, lógicamente siempre menores y se conocen en el mundo real.
- Medio. La situación de acoso siempre ocurre a través de dispositivos tecnológicos.
- Mensajería. Los mensajes contienen expresiones violentas como amenazas, insultos o difamaciones.
- Temporalidad. Un caso de ciberbullying se extiende en un plazo largo de tiempo. De lo contrario estaríamos ante un evento efímero de violencia verbal.

2.3.2.2. Grooming

Viaña de Avendaño (2016) aporta que:

> "Grooming" o "ciberacoso" son acciones deliberadas por parte de una persona adulta, hombre o mujer, con el propósito de establecer lazos de amistad con un niño o niña en internet; se crea una conexión emocional con el menor con el fin de disminuir las inhibiciones del mismo y poder abusar sexualmente de él. (p.2).

Todas estas acciones del acosador siguen un arquetipo de fases ampliamente conocido por las unidades policiales y los investigadores en ciberdelincuencia. Entre ellos se encuentra

Galence (2011), el cual señala claramente todos los pasos que, probablemente, siga un ciberdelincuente que cometa este delito.

- Contacto y acercamiento. El acosador emplea alguna red social o servicio de mensajería para contactar con el menor. Su objetivo es hacerse pasar por alguien menor de edad con aficiones similares, tratando de resultar atractivo a la víctima.
- Sexo virtual. El delincuente busca intimar con el menor en el transcurso de la relación, ganándose su confianza. En muchos casos logra obtener imágenes o vídeos con contenido sexual del niño o niña.
- Ciberacoso. En este punto ya no hay vuelta atrás, el acosador demanda mayores objetivos sexuales. En caso de no obtener lo deseado, este pasa a amenazar al adolescente con difundir los contenidos privados que tiene en su poder.
- Abuso-agresiones sexuales. El ciberdelincuente logra su objetivo, logrando abusar sexualmente en la vida real al menor.

2.3.2.3. Sexting

El término “sexting” hace mención del tipo de ciberacoso en el que existen envíos de contenido multimedia con carga sexual mediante dispositivos móviles. Esta práctica tan dañina para la intimidad se vuelve altamente peligrosa desde el momento en que se saca la foto, ya que conservar imágenes tan personales en un dispositivo con conexión a internet ya conlleva grandes riesgos. Sin embargo, el hecho de que pueda llegar a ser enviada está en un nivel de gravedad superior. De hecho, el potencial daño que puede sufrir la víctima depende de muchos factores técnicos, los cuales abordan Fajardo, Gordillo y Regalado (2013) con el objetivo de describir mejor las posibles situaciones de delitos denunciados de “sexting”. Estos aspectos son:

- El origen de la imagen. Puede haber sido realizada por la víctima o por otra persona (ya fuera con consentimiento o no).
- El contenido de la imagen. Graduación o nivel de carga sexual incluida en la imagen.
- La identificabilidad. Si puede reconocerse a la persona que sale en la imagen con facilidad.
- La edad del protagonista. No puede determinarse si la persona que sale en la foto es menor o mayor de edad, lo cual tiene gran relación con el punto anterior.

2.3.3. Peligros en la red IV: evasión de la propiedad intelectual

Si se analizan claramente las redes sociales, se visualizará que la mayoría de los mensajes y contenidos multimedia compartidos son provenientes de otras cuentas. Esto no es casualidad, ya que una de las principales funciones de un sitio web, que opere como plataforma social, es la divulgación instantánea y masiva de producciones de cualquier tipo. Como es obvio, en muchas ocasiones esto puede ser una ventaja para dar a conocer dicha elaboración, estableciendo una amplia cantidad de seguidores y contactos que estén atentos a futuras publicaciones. Pero, tal y como plantea Fariñas (2011), "muchas personas han malentendido la libertad de intercambio como una patente de corso para apropiarse impunemente de contenidos ajenos; para ellos intercambio es poder usar libremente, sin licencia previa, sin pago de remuneración alguna" (p.160). Como se puede llegar a imaginar, este factor de transmisión de datos a gran escala puede volverse en contra de cualquier creador de contenido o conocimiento. Y, tristemente, es extremadamente complejo establecer controles legales sobre toda la mensajería existente en todas las redes sociales, por no decir inviable. Desde luego, existen algoritmos pioneros en plataformas como Youtube, los cuales logran evitar muchas de las vulneraciones de propiedad intelectual, estableciendo denuncias automáticas ante esas infracciones. Esto es especificado por los autores Zalvide y Ramos (2020), los cuales afirman que "El sistema de Content ID fue creado como respuesta a las preocupaciones de las grandes compañías por vulneración de copyright y pérdida de beneficios" (p.3). Sin embargo, lo lógico no debe ser depender de estos sistemas, sino dar una formación en licencias y citación desde un nivel temprano en educación, fomentando el respeto a los materiales ajenos.

Por último, es relevante decir que este problema no nace a causa de las redes sociales, sino de una mala praxis humana. Sin embargo, este dilema debía relacionarse con estos programas por su aumento desmedido, lo cual se explica por la facilidad de difundir y compartir informaciones a través de estos medios.

3. Diseño de la propuesta didáctica

3.1. Contextualización

3.1.1. Descripción del centro educativo

El CEIP San Fernando se encuentra en la zona céntrica de Santa Cruz, muy cerca del estadio Heliodoro Rodríguez López y al lado del Barranco de Santos. Es un edificio muy antiguo, aunque posee construcciones anexas que son nuevas (las aulas que albergan a los grupos de Educación Infantil). El número total de aulas que alberga a todos los grupos-clase del centro es 19 (el centro cuenta con 19 tutorías, 6 de Educación Infantil y 13 de Educación Primaria). Todas las aulas disponen de un ordenador portátil para el docente, el cual cuenta con salida a una pizarra digital interactiva (PDI). Además, las aulas de quinto y sexto de Educación Primaria disponen de portátiles pertenecientes al Proyecto Escuela 2.0. (ordenadores portátiles para uso exclusivo del alumnado).

En cuanto al resto de instalaciones físicas del colegio, se ha tomado la decisión de plantear una estructura puntualizada con todos los espacios. Dicho esto, es momento de distinguir cada uno de ellos:

- Dos canchas al aire libre (30 metros de largo por 12 de ancho) como espacios de recreo.
- Un gimnasio en el cual se almacena el material de deportes.
- Un comedor con capacidad para 250 niños y niñas.
- No se dispone de salón de actos, en su defecto, el ayuntamiento cede las instalaciones del cine Víctor en fechas especiales.
- Una biblioteca, la cual es gestionada por ciertos representantes del alumnado.
- Un aula de informática con 20 ordenadores de mesa. El alumnado de quinto y sexto de primaria no suelen emplearla, ya que disponen de portátiles personales en sus clases.
- Un departamento que comparten la Asociación de Madres y Padres de Alumnos (AMPA) y los Equipos de Orientación Educativa y Psicopedagógicos (EOEP).

El número de estudiantes del centro educativo en el año 2019 era de 451, teniendo en cuenta las etapas de infantil y primaria. Estos datos han sido aportados por la directora del centro académico, además estarán representados claramente en una tabla segmentada con todas

las aulas (Anexo A). En cuanto a las características generales que pueden destacarse de toda esta población de menores, lo cierto es que la mayoría provienen del barrio Duggi de Santa Cruz (barrio de la escuela). Además, se cuenta con discentes de muchas nacionalidades: bolivianos, venezolanos, marroquíes, filipinos, ecuatorianos…Dada esta multiculturalidad, es evidente que el CEIP San Fernando tiene muchos elementos en su Programación General Anual (PGA) para fomentar la correcta inclusión de estos pequeños.

3.1.2. Destinatarios del Proyecto

El proyecto está destinado para la etapa de sexto de primaria del centro educativo (edades entre 11 y 12 años), es decir, se realizará a lo largo de tres cursos (6ºA, 6ºB y 6ºC). Se tiene en consideración una media de 25 niños y niñas por clase, es decir, unos 75 en totalidad. Los tutores de los tres cursos serán los únicos implicados en las áreas que afecten a la programación.

Este alumnado ha sido seleccionado como el destinatario por tres motivos:

- Los datos de uso de dispositivos e internet, presentados por el INE en 2020, muestran que los mayores incrementos son entre los 11 y los 12 años.
- Este es el curso (contando con la etapa infantil y primaria exclusivamente) con mayor número de talleres con relación a las redes sociales y la ciberseguridad.
- La competencia digital de estos menores se encuentra en un término de desarrollo más elevado por la formación anterior, lo cual admitirá un abanico mayor de procedimientos para las actividades.

3.2. Desarrollo del Proyecto

3.2.1. Objetivos y competencias básicas de la propuesta de innovación

Para iniciar los detalles que componen la programación del plan, se empezará detallando los objetivos que se han establecido.

A. Objetivo general. Generar comportamientos y pautas seguras en el mundo virtual.
B. Objetivos específicos:
    - ❖ Aplicar coherentemente un sistema de licencias de derechos de autor y una pauta de citado básica que garanticen el uso legal de los recursos ajenos.

- ❖ Clasificar los tipos de ciberacosos más comunes entre menores, relacionándolos a sus características principales.
- ❖ Analizar eficientemente los tipos de programas maliciosos y el nivel de seguridad de una página web.
- ❖ Utilizar las redes sociales siendo consciente de todos los métodos y condiciones que pueden llegar a configurarse.

3.2.2. Metodología

"Exploit City" es una gamificación dotada de unos contenidos extremadamente diversos del mundo de la seguridad en internet. No obstante, no se han comentado todos los detalles implicados en su creación. Esto tiene una razón coherente, y es que el entorno gamificado afecta directamente a la programación completa del proyecto, lo cual podrá verse claro en sus fases:

- Fase 1. Desarrollo basado en las propiedades intelectuales. En el comienzo se presentan conceptos y procedimientos relacionados con el uso de las licencias Creative Commons y los derechos de autor. Dentro de la narrativa este apartado guarda relación directa con la "Corporativa Commons".
- Fase 2. Desarrollo basado en el funcionamiento de tres tipos de ciberacoso y sus características. Ciberbullying, Sexting y Grooming serán puestos en análisis en las actividades que trabaje el alumnado. El nexo de estos peligros en la historia será la "Corporativa Tegra".
- Fase 3. Desarrollo basado en los tipos de virus, contenidos no deseados y las formas de protección ante los mismos. Todo estará acogido en la "Corporativa Black".
- Fase 4. Desarrollo basado en los apartados menos visibles de las redes sociales (configuración y términos de uso) y en sus consecuencias. Estos contenidos irán ligados a la "Corporativa Likers".

Cada una de esas corporativas (cuatro zonas propuestas en la gamificación) tendrá relacionados unos aprendizajes concretos sobre conductas seguras en internet, sin embargo, el motor de avance no será otro que el currículum. De esta forma, se lograrán integrar todos los aspectos altamente complejos del mundo digital en una programación basada en los criterios de evaluación.

Por otro lado, este diseño será revisado y evaluado en una evaluación triangular, la cual pretende validar la propuesta. Los tres vértices de esta valoración serán: dos docentes, un agente policial experto en ciberdelincuencia y su propio autor. Con este triple punto de vista es mucho más probable sacar resultados veraces.

"Exploit City" cuenta con una web de presentación en la que se presentarán todos estos detalles a familias y otros docentes.

3.2.3. Temporalización

La temporalización tendrá en cuenta los tiempos semanales de las áreas integradas en el proyecto: Matemáticas (6 sesiones), Lengua Castellana y Literatura (6 sesiones), Educación Artística (3 sesiones) y Ciencias Sociales (2 sesiones). En sexto de primaria, la combinación del total de sesiones de 55 minutos es de 18 a la semana. Sabiendo que cada semana se avanzará una fase de la gamificación, se ha desarrollado en la tabla 5 las actividades a trabajar en cada corporativa semanalmente. Es primordial recordar que la estructuración del horario también cambiará, ya que todas esas materias son impartidas por el mismo docente, que no es otro que el tutor. Señalado este hecho, se adjunta el cronograma de la propuesta.

Tabla 5. Cronograma de "Exploit City"

Fases de "Exploit City"	Actividades	Número de sesiones	Semana
Fase 1: Corporativa Commons	Symbaloo Creative Commons	4 sesiones	1º
	Protejamos nuestra infografía	3 sesiones	
	Citamos "todo, todo"	5 sesiones	
	AVANCE MATEMÁTICO (MAPA)	6 sesiones	
Fase 2: Corporativa Tegra	Lectura compresiva: Análisis de "Groomers"	2 sesiones	2º
	Adivina-teatros: ¿Ciberbullying o Sexting?	4 sesiones	
	E-book: Actuamos contra el ciberacoso	6 sesiones	

	AVANCE MATEMÁTICO (MAPA)	6 sesiones	
Fase 3: Corporativa Black	Especialistas en un virus: Presentamos a las familias	4 sesiones	3º
	Simulacro de ciberataque: ¿Estamos preparad@s?	2 sesiones	
	Diseñamos una web informativa: ¿Qué es una web segura?	6 sesiones	
	AVANCE MATEMÁTICO (MAPA)	6 sesiones	
Fase 4: Corporativa Likers	Lectura comprensiva: ¿Son las condiciones de uso una trampa?	3 sesiones	4º
	Configuración de las redes del curso "6ºX": Instagram, TikTok, Twitter, Facebook y Pinterest	3 sesiones	
	Iniciativa "Redundancia": Creemos carteles críticos de las redes sociales en las redes sociales	6 sesiones	
	AVANCE MATEMÁTICO (MAPA)	6 sesiones	

Fuente: Elaboración propia

3.2.4. Actividades

Las actividades de "Exploit City" estarán contenidas en un conjunto de tablas, las cuales tendrán que presentarse en una disposición horizontal y con otras condiciones de interlineado por necesidades logísticas textuales. Dicho esto, es importante indicar que todos los recursos estarán disponibles en el apartado de anexos correspondiente (Anexos E-N), destacando los de elaboración propia en todo momento.

Conjunto de tablas. Actividades de "Exploit City"

<table>
<tr><th colspan="7">Fase 1: Corporativa Commons</th></tr>
<tr><td colspan="7">1. Symbaloo Creative Commons</td></tr>
<tr><td colspan="7">Se establecerá un “Lesson Plan” en el que se integrarán distintos nodos a recorrer por el alumnado. En cada una de las posiciones habrá actividades relacionadas con las licencias Creative Commons (CC).
- El primer nodo contendrá un “Edpuzzle” explicativo con cuestiones introductorias o de apertura.
- El segundo nodo aportará una explicación y un enlace de entrega a “Google Drive” para un mapa conceptual (el discente lo hará con “Goconqr”).
- El tercer nodo incluirá 3 casos de personas (vídeos) que quieren ser asesoradas para elegir una licencia CC. Se responderá en un documento de texto.
El cuarto nodo es una autoevaluación basada en preguntas de Symbaloo, las cuales recogen las analíticas de cada menor.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PCS06C02
PEA06C04
Competencias:
AA, SIEE, CSC (CS)
CL, CD, CSC, CEC (EA)
Estándares de aprendizaje evaluables:
14, 16 (CS)
47 (EA)</td>
<td>Técnicas
Encuestación
Herramientas
Formulario de autoevaluación
Productos
-
Tipos de evaluación
Autoevaluación</td>
<td>Individual</td>
<td>4</td>
<td>- Recurso 1: 25 portátiles
- Recurso 2: Symbaloo (LP)
- Recurso 3: Edpuzzle
- Recurso 4: Goconqr
- Recurso 5: Documento Word
- Recurso 6: Google Drive
- Recurso 7: Vídeo 1
- Recurso 8: Vídeo 2
- Recurso 9: Vídeo 3</td>
<td>Aula</td>
<td>• Fomentar la valoración de la propiedad intelectual.
• Transmitir la importancia de las licencias Creative Commons en los productos creativos propios y ajenos.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 1: Corporativa Commons</th></tr>
<tr><td colspan="7">2. Protejamos nuestra infografía</td></tr>
<tr><td colspan="7">El alumnado creará una infografía, en la cual tendrán explicar correctamente el funcionamiento de cada una de las licencias Creative Commons y cómo se pueden utilizar en las creaciones intelectuales (explicar los pasos). Dicho recurso visual se realizará con “Piktochart for Teams”, teniendo que respetar una coherencia de colores y de proporciones entre las figuras o franjas utilizadas. Una vez hecho esto, el docente repartirá unas tarjetas que describirán una situación concreta, la cual describirá unas circunstancias que determinarán los permisos de uso de dichos productos visuales. Por tanto, este contexto determinará qué tipo de licencia debe asignar cada grupo a su infografía, explicando siempre el porqué de esa decisión.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PCS06C02
PEA06C01
Competencias:
AA, SIEE, CSC (CS)
AA, SIEE, CEC (EA)
Estándares de aprendizaje evaluables:
14, 16 (CS)
14, 18, 20 (EA)</td>
<td>Técnicas
Encuestación
Herramientas
Cuestionario de coevaluación 1
Productos
Infografía y su licencia
Tipos de evaluación
Coevaluación</td>
<td>Grupo cooperativo</td>
<td>3</td>
<td>- Recurso 1: 25 portátiles
- Recurso 10: Piktochart
- Recurso 11: Tarjetas</td>
<td>Aula</td>
<td>• Producir productos artísticos haciendo un uso eficiente del color y la proporción.
• Transmitir la importancia de las licencias Creative Commons en los productos creativos propios y ajenos.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 1: Corporativa Commons</th></tr>
<tr><td colspan="7">3. Citamos “todo, todo”</td></tr>
<tr><td colspan="7">Los grupos cooperativos tendrán que elegir un tema de rigor de elección libre (puede ser histórico, científico, artístico, etc.). Este tópico será el centro de una investigación pautada (habrá una guía a seguir), en la cual tendrán que citarse 10 autorías distintas de documentos o de recursos audiovisuales con la siguiente estructura de citado: “Nombre del autor/a o de los autores, Año, Nombre del documento o recurso, Nombre de la fuente (libro, revista, blog, web…). Enlace web”. El objetivo es establecer que pueden emplearse productos de otros, siempre y cuando exista un respeto y reconocimiento a su trabajo.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C04
PCS06C02
Competencias:
CL, AA, CEC, CD (LCL)
AA, SIEE, CSC (CS)
Estándares de aprendizaje evaluables:
30, 61, 64, 72, 73, 74, 75 (LCL)
14, 16 (CS)</td>
<td>Técnicas
Análisis de documentos
Herramientas
Rúbrica 1
Productos
Investigación grupal
Tipos de evaluación
Heteroevaluación</td>
<td>Grupo cooperativo</td>
<td>5</td>
<td>- Recurso 1: 25 portátiles
- Recurso 6: Google Drive
- Recurso 12: Google Scholar
- Recurso 13: Guía</td>
<td>Aula</td>
<td>• Introducir el uso de mecanismos de citación (simplificados).
• Adquirir hábitos y expresiones correctas de escritura (adecuadas al nivel), respetando todas las normas de estructura, ortografía y puntuación.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 2: Corporativa Tegra</th></tr>
<tr><td colspan="7">4. Lectura comprensiva: Análisis de “Groomers”</td></tr>
<tr><td colspan="7">El alumnado tendrá que afrontar distintas conversaciones de Whatsapp simuladas, en las cuales podrán visualizarse claramente distintas conductas propias de las fases del Grooming. El objetivo es que cada educando conteste una serie de cuestiones y preguntas individualmente, y posteriormente, realicen una técnica 1-2-4 (puede existir variación de la técnica 1-2-4 por el tamaño de los grupos cooperativos) para poner en común el análisis comprensivo de las situaciones de Grooming. Al final, entregarán un análisis en conjunto del grupo, incluyendo también los de los integrantes.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C03
Competencias:
CL, AA, CEC
Estándares de aprendizaje evaluables:
44, 50, 52</td>
<td>Técnicas
Encuestación
Herramientas
Formulario de autoevaluación
Productos
Análisis de preguntas grupal y de integrantes
Tipos de evaluación
Autoevaluación</td>
<td>Individual

Pareja

Grupo cooperativo</td>
<td>2</td>
<td>- Recurso 1: 25 portátiles
- Recurso 14: Fichas de cuestiones con conversaciones de WhatsApp simuladas</td>
<td>Aula</td>
<td>• Mejorar todos los procesos y razonamientos intervinientes en la comprensión lectora.
• Comprender el funcionamiento, fases, protocolos de defensa y recursos ante el ciberacoso (Grooming).</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 2: Corporativa Tegra</th></tr>
<tr><td colspan="7">5. Adivina-teatros: ¿Ciberbullying o Sexting?</td></tr>
<tr><td colspan="7">El alumnado recibirá una explicación breve del docente sobre dos tipos de ciberacoso: sexting y ciberbullying. Tras esto, indicará a los grupos cooperativos que tendrán que diseñar un guion teatral de una extensión máxima de 4 caras. Además, podrán emplear los teléfonos móviles en la obra (los cuales serán monitorizados con “Teamviewer” con el objetivo de que el resto de los grupos puedan visualizar las conversaciones en directo). El objetivo es que el resto de los grupos adivinen qué tipo de ciberacoso se dramatizaba. Además, darán posibles soluciones y recursos defensivos en debate tras cada teatrillo. Por último, cada grupo evaluará a todos los grupos, exceptuando al suyo, ya que se busca obtener una perspectiva del público en todo momento.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C07
PCS06C03
Competencias:
CL, AA, SIEE, CEC (LCL)
CSC, SIEE, CEC (CS)
Estándares de aprendizaje evaluables:
19, 104 (LCL)
11, 12, 13 (CS)</td>
<td>Técnicas
Encuestación
Herramientas
Cuestionario de coevaluación 2
Productos
Representación teatral
Tipos de evaluación
Coevaluación</td>
<td>Grupo cooperativo</td>
<td>4</td>
<td>- Recurso 15: Vestuario (casa del alumnado)
- Recurso 16: Cartón (Decorado)
- Recurso 17: Móviles del alumnado
- Recurso 18: Teamviewer</td>
<td>Aula</td>
<td>• Comprender el funcionamiento, protocolos de defensa y recursos ante el ciberacoso (Sexting y Ciberbullying).
• Desarrollar habilidades escénicas y dramáticas propias de la actividad teatral.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 2: Corporativa Tegra</th></tr>
<tr><td colspan="7">6. E-book: Actuamos contra el ciberacoso</td></tr>
<tr><td colspan="7">Los grupos tendrán que realizar un E-book o una infografía que explique de forma básica lo aprendido sobre los tres tipos de ciberacoso trabajados. Este recurso debe ser visualmente atractivo y tener un lenguaje y expresión adecuada para ser compartido con toda la comunidad educativa (se alojará en Issuu).</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C04
PCS06C03
PEA06C01
Competencias:
CL, AA, CEC, CD (LCL)
CSC, SIEE, CEC (CS)
AA, SIEE, CEC (EA)
Estándares de aprendizaje evaluables:
60, 61, 75 ,76 (LCL)
11, 17 (CS)
14, 18, 20 (EA)</td>
<td>Técnicas
Análisis de documentos
Herramientas
Rúbrica 2
Productos
E-book de cada grupo
Tipos de evaluación
Heteroevaluación</td>
<td>Grupo cooperativo</td>
<td>6</td>
<td>- Recurso 1: 25 portátiles
- Recurso 10: Piktochart
- Recurso 19: Canva
- Recurso 20: Issuu</td>
<td>Aula</td>
<td>• Comprender el funcionamiento, protocolos de defensa y recursos ante el ciberacoso (Sexting, Ciberbullying y Grooming).
• Producir productos artísticos haciendo un uso eficiente del color y la proporción.
• Respetar el formato de escritura, contando con las normas de ortografía y puntuación.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 3: Corporativa Black</th></tr>
<tr><td colspan="7">7. Especialistas en un virus: Presentamos a las familias</td></tr>
<tr><td colspan="7">El alumnado de los grupos se volverá experto en un tipo de malware, del cual tendrá que hacer una presentación al resto de la clase. Los tipos para repartir entre los grupos son: Troyano, Gusano, Virus en spam, Phishing y Botnet. Las diapositivas deberán explicar los siguientes detalles: “Descripción del programa malicioso”, “Funcionamiento”, “Información en peligro”, “Ejemplos de ataques” y “Métodos o barreras defensivas”. Todos estos detalles serán comunicados a las familias en el salón de actos del centro educativo, los cuales tendrán el papel de evaluar esta tarea en conjunto con los grupos.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C02
Competencias:
CL, AA, CSC
Estándares de aprendizaje evaluables:
1, 2, 6, 7, 25, 26</td>
<td>Técnicas
Encuestación
Herramientas
Cuestionario de coevaluación 3
Productos
Presentación
Tipos de evaluación
Coevaluación</td>
<td>Grupo cooperativo</td>
<td>4</td>
<td>- Recurso 1: 25 portátiles
- Recurso 21: Genial.ly</td>
<td>Aula

Salón de actos</td>
<td>• Concebir los tipos de malware y sus características principales, incluyendo métodos de defensa.
• Crear situaciones guionizadas de comunicación oral, dando valor a todos los aspectos intervinientes en ella.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 3: Corporativa Black</th></tr>
<tr><td colspan="7">8. Simulacro de ciberataque: ¿Estamos preparad@s?</td></tr>
<tr><td colspan="7">El alumnado explorará individualmente un tipo de virus: troyanos. No obstante, estos virus en ningún caso tendrán funcionalidades invasivas o peligrosas, tan solo realizarán actos simples como apagado o reinicio de ordenador, abrir numerosas ventanas, dar un mensaje inofensivo…El objetivo es rellenar una ficha de registro del virus, en la cual tengan que contestarse a una serie de apartados (tipo de virus, sistema de ocultación, función de ataque, método de detección usado y peligros potenciales del tipo de malware trabajado). Se explicará bien el uso de “Propiedades” (click derecho) por parte del docente, como método de evitación de troyanos (además del antivirus) y, por supuesto, formas de evitar correo malintencionado.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C04
Competencias:
CL, AA, CEC, CD
Estándares de aprendizaje evaluables:
61, 74, 75</td>
<td>Técnicas
Encuestación
Herramientas
Formulario de autoevaluación
Productos
Ficha de registro
Tipos de evaluación
Autoevaluación</td>
<td>Individual</td>
<td>2</td>
<td>- Recurso 1: 25 portátiles
- Recurso 22: Ficha de trabajo
- Recurso 23: Virus (troyanos)
- Recurso 24: Ficheros de los virus</td>
<td>Aula</td>
<td>• Concebir los tipos de malware y sus características principales, incluyendo métodos de defensa.
• Respetar el formato de escritura, contando con las normas de ortografía y puntuación.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 3: Corporativa Black</th></tr>
<tr><td colspan="7">9. Diseñamos una web informativa: ¿Qué es una web segura?</td></tr>
<tr><td colspan="7">En ciertas ocasiones la entrada o acceso a una web puede llegar a suponer un grave problema de seguridad para los usuarios, ya que no siempre se navega por una red plenamente segura. El objetivo de esta actividad es crear una página con Google Sites, incluyendo 4 secciones o páginas: “Indicadores de web segura”, “Información veraz online”, “Protocolo HTTP vs HTTPS” y “¿Quiénes somos?” (describiendo los integrantes del grupo). Toda la información y multimedia tendrá que ser citada correctamente para respetar la propiedad intelectual. Las webs serán compartidas con la comunidad del centro.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C04
PEA06C01
Competencias:
CL, AA, CEC, CD (LCL)
AA, SIEE, CEC (EA)
Estándares de aprendizaje evaluables:
60, 64, 76 (LCL)
14, 18, 20 (EA)</td>
<td>Técnicas
Análisis de documentos
Herramientas
Rúbrica 3
Productos
Página web
Tipos de evaluación
Heteroevaluación</td>
<td>Grupo cooperativo</td>
<td>6</td>
<td>- Recurso 1: 25 portátiles
- Recurso 25: Google Sites</td>
<td>Aula</td>
<td>• Entender los distintos elementos que convierten una web en un espacio seguro y de información veraz.
• Producir productos artísticos haciendo un uso eficiente del color y la proporción.
• Respetar el formato de escritura, contando con las normas de ortografía y puntuación.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 4: Corporativa Likers</th></tr>
<tr><td colspan="7">10. Lectura comprensiva: ¿Son las condiciones de uso una trampa?</td></tr>
<tr><td colspan="7">Los integrantes de cada grupo recibirán un enlace para unas condiciones de uso de una red social (por ejemplo, todos los participantes del grupo A reciben las condiciones de Pinterest). El objetivo es que se resuelvan una serie de cuestiones que permitan hacer una búsqueda de información clave en un gran texto, obteniendo una idea básica de muchas de las bases legales que se aceptan al usar una red social. Esta tarea es clave para el desarrollo posterior de la actividad 11, la cual está muy vinculada con esta.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PLCL06C03
PCS06C08
Competencias:
CL, AA, CEC (LCL)
AA, CSC, SIEE, CD, CL (CS)
Estándares de aprendizaje evaluables:
34, 35, 36, 42, 50 (LCL)
70 (CS)</td>
<td>Técnicas
Encuestación
Herramientas
Formulario de autoevaluación
Productos
Ficha de cuestiones
Tipos de evaluación
Autoevaluación</td>
<td>Individual</td>
<td>3</td>
<td>- Recurso 1: 25 portátiles
- Recurso 26: Condiciones de uso de Twitter
- Recurso 27: Condiciones de uso de TikTok
- Recurso 28: Condiciones de uso de Pinterest
- Recurso 29: Condiciones de uso de Instagram
- Recurso 30: Condiciones de uso de Facebook
- Recurso 31: Ficha de cuestiones</td>
<td>Aula</td>
<td>• Mejorar todos los procesos y razonamientos intervinientes en la comprensión lectora.
• Establecer unas nociones realistas de los usos de las redes sociales, sus configuraciones y sus condiciones (protección de datos, anuncios, multimedia...).</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 4: Corporativa Likers</th></tr>
<tr><th colspan="7">11. Configuración de las redes del curso “6ºX”: Instagram, TikTok, Twitter, Facebook y Pinterest</th></tr>
<tr><td colspan="7">El docente aportará una cuenta e-mail de la clase de 6ºA, la cual será aportada a todos los grupos cooperativos. Cada grupo tendrá que crear una red social llamada “Clase Sexto Curso del CEIP San Fernando” (o nombres similares) de la red que trabajaran en la actividad anterior. El objetivo de la actividad es promocionar un futuro evento de cartelería, el cual se realizará en la actividad siguiente. Por ello, tendrán que administrarse esas redes sociales en cada grupo, tratando de aplicar técnicas publicitarias. Es importante tener en cuenta las características únicas de cada red, promoviendo además un uso seguro y adecuado de las mismas. Por este motivo, cada grupo recibirá una hoja de instrucciones con la configuración adecuada y la ruta a seguir en la promoción.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PCS06C08
Competencias:
AA, CSC, SIEE, CD, CL
Estándares de aprendizaje evaluables:
70</td>
<td>Técnicas
Encuestación
Herramientas
Cuestionario de coevaluación 4
Productos
Perfiles de las redes
Tipos de evaluación
Coevaluación</td>
<td>Grupo cooperativo</td>
<td>3</td>
<td>- Recurso 1: 25 portátiles
- Recurso 17: Móviles del alumnado
- Recurso 32: Cuenta e-mail
- Recurso 33: Instrucciones del grupo Twitter
- Recurso 34: Instrucciones del grupo TikTok
- Recurso 35: Instrucciones del grupo Pinterest
- Recurso 36: Instrucciones del grupo Instagram
- Recurso 37: Instrucciones del grupo Facebook</td>
<td>Aula</td>
<td>• Establecer unas nociones realistas de los usos de las redes sociales, sus configuraciones y sus condiciones (protección de datos, anuncios, multimedia…).
• Promover el uso de estrategias publicitarias y del mundo del marketing.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Fase 4: Corporativa Likers</th></tr>
<tr><td colspan="7">12. Iniciativa “Redundancia”: Creemos carteles críticos de las redes sociales en las redes sociales</td></tr>
<tr><td colspan="7">El alumnado debe desarrollar un cartel creativo que exprese un gran hecho crítico de la red utilizada. Por tanto, cada grupo debe hacer su propio cartel cooperativamente. Dichos carteles deberán tener muchos elementos (figuras, líneas, iconos, personajes, letras…), y todos ellos deben ser libres de derechos de autor. Dicho esto, el objetivo es difundir todos esos carteles en las redes creadas, generando una pequeña “expo”, la cual se llamará “Redundancia”. Es importante indicar que todos estos carteles deben tener una licencia CC BY-NC-ND, protegiendo de forma total los carteles.</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PEA06C01
PEA06C02
Competencias:
AA, SIEE, CL, CD, CEC
Estándares de aprendizaje evaluables:
6, 10, 12, 14, 18, 20</td>
<td>Técnicas
Análisis de documentos
Herramientas
Rúbrica 4
Productos
Carteles
Tipos de evaluación
Heteroevaluación</td>
<td>Grupo cooperativo</td>
<td>6</td>
<td>- Recurso 1: 25 portátiles
- Recurso 10: Piktochart
- Recurso 19: Canva
- Recurso 21: Genial.ly
- Recurso 32: Cuenta e-mail</td>
<td>Aula</td>
<td>• Entender los hechos negativos que incluyen las redes sociales, visibilizando y difundiendo su impacto en la sociedad digital.
• Producir productos artísticos haciendo un uso eficiente del color y la proporción.
• Generar efectos de difusión a través del uso de carteles artísticos.</td>
</tr>
</table>

<table>
<tr><th colspan="7">Actividad común a todas las fases (1,2,3 y 4)</th></tr>
<tr><td colspan="7">13. AVANCE MATEMÁTICO (MAPA)</td></tr>
<tr><td colspan="7">Esta actividad forma parte del sistema de juego de la gamificación. Tras lanzar el dado de 4 de rol, según el resultado se establece una tipología de problemas u operaciones (1 – Potencias, 2 – Jerarquía de operaciones, 3 – Porcentajes (cálculo y regla de 3), 4 – Decimales y fracciones). Cada vez que se localice o encuentre enemigos en los mapas de las corporativas tendrá que lanzarse ese dado, decidiendo las operaciones a realizar. La condición principal es que todo el grupo al completo debe acertar en el resultado si se quiere atacar (resultado correcto permite atacar), y por ello, se permiten ayudas entre integrantes del equipo (nunca compartir el resultado, ya que es motivo de penalización).</td></tr>
<tr><th>Cod. CE
Compet.
Estándares</th><th>Técnicas
Herramientas
Productos
Tipos de evaluación</th><th>Agrupamientos</th><th>Sesiones</th><th>Recursos</th><th>Espacios</th><th>Objetivos</th></tr>
<tr>
<td>Código:
PMAT06C04
PMAT06C05
Competencias:
CL, CMCT, AA
Estándares de aprendizaje evaluables:
4, 34, 36, 38, 41 50, 53, 54, 55, 63, 65</td>
<td>Técnicas
Análisis de documentos
Herramientas
Cuestionario de coevaluación 5
Productos
Operaciones y problemas recopilados del grupo
Tipos de evaluación
Coevaluación</td>
<td>Grupo cooperativo</td>
<td>24
(6 por cada fase)</td>
<td>- Recurso 33: Dados de rol del grupo
- Recurso 34: Banco de operaciones y problemas</td>
<td>Aula</td>
<td>• Mejorar los procesos involucrados en la resolución de problemas simulados o reales.
• Optimizar y depurar el cálculo operacional en múltiples formatos numéricos (porcentajes, decimales, fracciones, sistema numérico decimal…</td>
</tr>
</table>

Fuente: Elaboración propia

3.2.5. Evaluación de la propuesta didáctica

La evaluación del proyecto estará clarificada en la tabla 6, la cual dejará patente el valor total de "Exploit City" (10 puntos). Es importante dejar claro que la gamificación no tiene efectos cualitativos ni cuantitativos en este caso, ya que se considera que su único papel es ser el motor lúdico del proceso de enseñanza-aprendizaje.

Tabla 6. Distribución porcentual de la evaluación

Evaluación	Actividades	Herramientas de evaluación
Heteroevaluación 60%	Actividad 3 (15%)	Rúbrica 1 (Anexo B)
	Actividad 6 (15%)	Rúbrica 2 (Anexo B)
	Actividad 9 (15%)	Rúbrica 3 (Anexo B)
	Actividad 12 (15%)	Rúbrica 4 (Anexo B)
Coevaluación 30%	Actividad 2 (2,5%)	Cuestionario de coevaluación 1 (Anexo C)
	Actividad 5 (2,5%)	Cuestionario de coevaluación 2 (Anexo C)
	Actividad 7 (2,5%)	Cuestionario de coevaluación 3 (Anexo C)
	Actividad 11 (2,5%)	Cuestionario de coevaluación 4 (Anexo C)
	Actividad 13 (20%)	Cuestionario de coevaluación 5 (Anexo C)
Autoevaluación 10%	Actividad 1 (2,5%)	Formulario de autoevaluación (Anexo D)
	Actividad 4 (2,5%)	
	Actividad 8 (2,5%)	
	Actividad 10 (2,5%)	

Fuente: Elaboración propia

3.2.6. Medidas de atención a la diversidad

"Exploit City" tiene lugar, en su práctica totalidad, en los ordenadores o portátiles en los que trabaje el alumnado. Dadas estas circunstancias, lo cierto es que existen dos tipologías de sintomatologías que pueden afectar tremendamente al aprendizaje del alumnado, llevando al punto de usar software o hardware específicos para trabajar de forma óptima.

- Diversidad funcional de modalidad visual. Aquellos educandos que tengan dificultades para la visión, lo cual pueda complicar el seguimiento de muchos de los recursos del proyecto. Estos son los apoyos que podrán usarse para fomentar su correcta integración en el trabajo curricular:
    - ❖ Magnificador de pantalla. Para casos de ceguera parcial o problemas de vista comunes pueden usarse comandos como "Control + Rueda del ratón" para ampliar recursos en pantalla, ya sea momentánea o permanentemente.
    - ❖ Lector de pantalla. En situaciones de ceguera total se emplearán programas como Job Access With Speech (JAWS) o VoiceOver (iOS), los cuales aseguran la accesibilidad a los distintos elementos con los que el discente pueda interactuar en su pantalla.
    - ❖ Impresora braille. Todos aquellos recursos textuales que se necesiten serán traducidos y, posteriormente, impresos con una impresora aportada por la Organización Nacional de Ciegos Españoles (ONCE).
- Diversidad funcional de modalidad sonora.
    - ❖ Transcriptor de audio. El alumnado dispondrá de programas como Dictation (ordenador) o ListenAll (móviles) para hacer una transcripción completa de las explicaciones del docente. No obstante, lo óptimo es disponer de un profesional formado plenamente en lenguaje de signos, pero esta alternativa puede ayudar en caso de no disponer de uno.
    - ❖ Uso de Youtube para subtítulos. Todos los vídeos subidos en esta plataforma cuentan con subtítulos generados que pueden favorecer la comprensión completa de los recursos multimedia del proyecto.

Evidentemente, más allá de estos posibles casos, también pueden encontrarse adaptaciones curriculares por desfase de nivel en ciertas áreas o por diversidades funcionales de carácter cognitivo. No obstante, estas no presentan tantos problemas como las contadas previamente.

3.2.7. Recursos especiales de la gamificación

Para finalizar con la presentación de la propuesta didáctica hace falta detallar claramente el conjunto de recursos y materiales que componen la gamificación "Exploit City". En primer lugar, es necesario precisar que todos y cada uno de los mismos han sido realizados por el autor del proyecto. Evidentemente, haciendo uso de plataformas de edición y diseño. En la tabla 7 pueden contemplarse los recursos elaborados en función de cada herramienta, incluyendo además sus anexos:

Tabla 7. Relación entre plataformas y recursos

Plataformas	Recursos	Anexos
Canva	Logotipo de Exploit City (GIF)	Anexo Q
	Logotipo de Exploit City	Anexo Q
	Medalla del juego	Anexo Q
Adobe Premiere	Vídeo de presentación	Anexo Q
Dungeonfog (DGNFOG)	Mapas	Anexo Q
	Enemigos habituales	Anexo Q
Wix	Web de presentación	Anexo Q
Office	Manual de la gamificación	Anexos P y Q

Fuente: Elaboración propia

Además de esos recursos, en el anexo de enemigos se incluyen unos "Jefes finales" que no han sido realizados con ninguna plataforma, ya que cuatro imágenes son tomadas de la red (libres de derechos) y la otra es una imagen del autor del TFE personalizada. Esta ha sido encargada para este objetivo, por tanto, se poseen derechos plenos sobre ella. Por último, se destacan los dados de rol como el único recurso físico (Anexo O).

4. Evaluación técnica del proyecto

Antes de iniciar el análisis de la evaluación externa del proyecto, es primordial agradecer la participación de los distintos profesionales en la propuesta. Concretamente se transmiten estos agradecimientos a dos docentes de Educación Primaria (pertenecientes a distintos centros educativos) y a un policía nacional experto en detalles y casos en ciberdelincuencia. Sus puntos de vista darán un rigor y unos márgenes de mejora incuestionables. Como extra, también se empleará el mismo instrumento de valoración de los docentes por parte del autor. Esto se hará con el objetivo de autoevaluar usando las mismas bases por parte del sector educativo. Dicho esto, es la hora de afrontar los datos aportados por todos los agentes.

4.1. Método de valoración

El presente punto introducirá como método de obtención de datos la encuesta por medio de cuestionarios. Estos formularios y sus respuestas estarán disponibles en los anexos (Anexos R-T). Estas herramientas valorativas se han diseñado tratando de abordar las distintas dimensiones del proyecto, llegando a compatibilizar la mayoría de las cuestiones para los dos sectores (educativo y policial). No obstante, existen cuatro preguntas añadidas para los docentes. Estas tratan aspectos concretos de la propuesta didáctica (actividades, recursos, evaluación y atención a la diversidad).

La mejor cualidad de este sistema se concentra en contemplar la visión que tienen los expertos con respecto a la colaboración de las fuerzas de seguridad del Estado y el sector educativo. Esto es un punto clave, ya que “Exploit City” en ningún caso pretende sustituir el trabajo divulgativo y educativo hecho por la policía u otros educadores externos. Al contrario, la idea es que se creen paralelismos y secuenciaciones que hagan ver la ciberseguridad en la red como el único camino posible. Esto solamente será posible con cooperación entre los profesionales, por ello, se hará hincapié en estos datos en el análisis.

4.2. Análisis de los resultados

Dados los resultados de las encuestas solamente queda abordar las ideas que subyacen bajo cada respuesta. Para hacerlo, se establecerá una taxonomía en grupos de preguntas que permitirá contrastar mejor la opinión de todos los expertos:

- Preguntas de identificación (Preguntas 1 - 3).
    - ❖ Policía. Este profesional realiza la comunicación más delicada de datos, ya que tiene que comunicar su número de placa con el objetivo de acreditar su posición de policía nacional.
    - ❖ Docentes. Estos profesionales comunican sus centros de trabajo y sus ámbitos de docencia, los cuales coinciden con el autor del proyecto.
    - ❖ Autoevaluación. Al ejecutar el mismo cuestionario que los docentes debe indicarse que no procede indicar centro de trabajo y, desde luego, que es una autoevaluación en los mismos términos (mismas preguntas).
- Preguntas de conveniencia de la propuesta (Preguntas 4 - 7).
    - ❖ Policía. El agente valora la importancia de tratar la temática y los contenidos de "Exploit City" dentro de la escuela, ya que se considera que en la franja de edad de sexto curso de primaria se dispara el uso de los dispositivos. De hecho, apoya la premisa de trabajar estos aspectos haciendo uso del conocimiento docente y de metodologías lúdicas como la gamificación. No obstante, debe contarse con la presencia y la opinión de las fuerzas de seguridad del Estado para abordar cualquier proyecto de esta dimensión.
    - ❖ Docentes. Ambos docentes valoran la necesidad de integrar contenidos del área de ciberseguridad en la escuela, y especialmente en estas edades. Sin embargo, no consideran primordial la presencia ni la valoración de agentes policiales. En otras palabras, el docente puede trabajar estos aspectos por su cuenta.
    - ❖ Autoevaluación. La opinión del autor coincide completamente con la del policía. Es decir, es primordial coordinar a los profesionales de ambos sectores para conseguir un mejor resultado en la modificación de las conductas en la red.
- Preguntas de validez de las actividades (Preguntas 8 - 15).
    - ❖ Policía. Todas las fases y sus actividades cumplen con los estándares de calidad del agente (teniendo en cuenta que fueron vistas por el mismo con una explicación del autor). A pesar de ello, considera que dos de las fases (Commons y Tegra) necesitan un especial cuidado en la formación del docente y en la presencia de expertos externos que lo apoyen en el desarrollo.

- ❖ Docentes. Ambos docentes consideran muy adecuadas las actividades. De hecho, su opinión es que cada fase logrará corregir cada conducta en la red en el alumnado (respeto a las licencias digitales y derechos de autor, análisis y recursos ante el ciberacoso, protección ante malware o software maligno y uso correcto de redes sociales). Además, consideran que con el trabajo docente ya es suficiente para lograrlo.
- ❖ Autoevaluación. Nuevamente la opinión del autor coincide con la del policía. A pesar de que, en general, todos los agentes están de acuerdo en el correcto diseño de las actividades para lograr las conductas en ciberseguridad, el autor no considera que pueda diluirse el papel de las fuerzas de seguridad del Estado. Es posible que puedan lograrse mejoras de forma independiente, pero nunca podrá lograrse los mismos resultados que en una situación de coordinación coherente entre especialistas.

- Preguntas de consecución de objetivos (Preguntas 16 - 18).
  - ❖ Policía. Este experto considera que "Exploit City" puede disminuir el número de delitos virtuales, estando además el alumnado protegido ante estas faltas legales por sus nuevas conductas seguras en la red. No obstante, dada a su posición en el cuerpo y su conocimiento estructural del mismo, él considera que es poco probable que haya un aumento de las denuncias de estos delitos. Esto conlleva que no se reduzca la cifra negra de denuncias.
  - ❖ Docentes. Ambos docentes consideran que los delitos virtuales podrán reducirse si se aplica este proyecto y, por supuesto, se conseguirá aumentar el número de denuncias de esta tipología de crímenes. Además, consideran que el objetivo principal del proyecto, que no es otro que generar unas conductas ciberseguras, también se cumplirá.
  - ❖ Autoevaluación. El autor no se muestra tan seguro en el impacto legal del proyecto. Según su opinión, las denuncias y los delitos pueden sufrir variaciones positivas si se comenzara a implementar "Exploit City", pero la realidad es que estas cifras solamente han sufrido cambios negativos hasta ahora. No obstante, sí cree en la potencia del trabajo como motor de cambio de conductas en la red.

- Preguntas de diseño curricular (Preguntas 19 - 22, solo docentes).
    - ❖ Docentes. Ambos docentes dan su aval de la calidad de la propuesta didáctica, destacando las actividades, sus recursos, su evaluación y los medios preparados para abordar alumnado de diversidad funcional. Mientras se supere el valor intermedio, se toma como factor positivo de la programación.
    - ❖ Autoevaluación. El autor coincide con los dos profesionales educativos en activo. Todos los elementos parecen ser adecuados para la consecución de los objetivos propuestos.

4.3. Conclusiones

Una vez afrontadas las valoraciones, queda acreditada una de las principales metas de esta propuesta de innovación, la cual es asegurar que, si algún profesional educativo lleva a cabo "Exploit City" en un centro con características similares al CEIP San Fernando, se conseguirá mejorar las conductas en la red del alumnado. Debe recordarse que estos discentes se encontraban completamente solos en sus primeros pasos en el mundo digital, y lo más probable es que muchas otras aulas se produzcan situaciones similares.

En un nivel jerárquico menor de objetivos, también puede verse que las aportaciones de este proyecto pueden ser de una elevada utilidad divulgativa. Especialmente en la combinación de los contenidos curriculares con dilemas como el ciberacoso o el uso de las redes sociales, ya que esto a priori puede parecer imposible para un docente. Las distintas aportaciones de investigadores en educación y ciberseguridad dejan clara la posibilidad de mezclar sus distintas temáticas. Y, además, se cuenta con un amplio abanico de actividades y materiales que desarrollan de manera práctica esta idea.

En cuanto al uso de la gamificación como enfoque metodológico principal de la experiencia, deben retomarse las ideas aportadas por los expertos que valoraron el proyecto. Todos coinciden en que el alumnado puede ponerse a la defensiva si se trata de coartar o limitar su libertad de uso de internet. Esto tiene una explicación biológica y otra de carácter social. Por un lado, en estas edades las enseñanzas de los adultos pueden causar conductas de rechazo al aprendizaje (más aún si no son personas de su confianza). Y, por otro lado, es complicado aceptar limitaciones por imposición. De aquí nace la necesidad de usar metodologías de enseñanza que aporten dichos conocimientos de una forma más amena y divertida.

Como conclusión, es primordial decir que para manejar eficientemente todas estas metas se necesitan poseer unas competencias digitales como maestro o maestra. Es imposible dotar al educando de una mente preparada y eficaz ante los peligros de internet si el docente no dispone de dicha psique también. Todo educador debe esforzarse en ser un experto en el ciberespacio, ya que solo así podrán aportarse las herramientas para que todo menor logre serlo.

4.4. Limitaciones y prospectiva

Para finalizar este proyecto de innovación se darán a conocer las distintas dificultades que se han encontrado en su elaboración. Esto servirá como material de consulta para todos aquellos que deseen realizar una nueva propuesta en esta línea de investigación. Principalmente, estos han sido los obstáculos:

- Imposibilidad de puesta en práctica. Obviamente el hecho de no poseer un aula para ejecutar la propuesta imposibilita obtener una valoración idónea de las actividades diseñadas. Esto conlleva buscar un aval distinto de la calidad del trabajo, y en el caso de "Exploit City" hay varias temáticas involucradas. De aquí la importancia de incluir expertos de cada área. Como puede imaginarse, esta no es una tarea sencilla.
- Creación de ciertos materiales propios. En el caso concreto de la gamificación, es cierto que pueden usarse recursos pertenecientes a otros y otras, pero esto genera muchas posibilidades de vulnerar ciertos derechos de autoría si no se hace un correcto análisis. De esta tesitura nace la necesidad de crear la totalidad de los recursos (exceptuando cuatro imágenes y una canción libres de derechos) para el entorno gamificado. Esta puede ser una misión dura sin un conocimiento amplio de herramientas digitales de creación de contenidos. Por suerte, este no fue el caso de este trabajo.
- Conexión entre contenidos curriculares y aspectos de ciberseguridad. En muchas ocasiones es complicado conectar un centro de interés con el currículum, esto no es novedad. No obstante, la ciberseguridad eleva esta dificultad de diseño programático exponencialmente.

Teniendo estas complejidades en mente es altamente posible que futuras investigaciones partan de una mejor posición que la de este TFE. Posiblemente logren ampliar y mejorar muchos de los detalles expuestos en los anteriores puntos. Como recomendación técnica para

futuros y futuras docentes, sería conveniente abordar las relaciones existentes entre la reputación y la identidad digitales haciendo uso de la gamificación. Esta realidad no ha sido abordada en “Exploit City” y lo cierto es que guarda una relación estrecha con la ciberseguridad. Sería interesante ver conclusiones de proyectos que fundamentaran dicha conexión haciendo uso de este TFE. Esto sería todo un honor para su autor, ya que implicaría que otros y otras en su gremio creen en la misma forma de enseñar.

Referencias bibliográficas

Arpí, C., Àvila, P., Baraldés, M., Benito, H., Gutiérrez, M. J., Orts, M., y Rostán, C. (2012). El ABP: origen, modelos y técnicas afines. *Aula de innovación educativa,* 216, 14-18.

Avogadro, M. (2009). Comunicación, redes sociales y ciberdelitos. *Razón y Palabra.* https://bit.ly/2R9xkJa

Bartle, R. A. (2008). *Player types* [Diapositivas de PowerPoint]. https://bit.ly/2QBrIrq

Bermúdez, R. A. (2005). *Diseño de un método de prevención y detección de virus gusano para mitigar el impacto económico y mantener la productividad al ser implementado en las universidades de México*. Instituto Tecnológico y de Estudios Superiores de Monterrey.

Brody, R. G., Mulig, E., y Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting & Financial Studies Journal,* 11(3), 43-56.

Cepeda, L. M. (2019). *Ciberpadres 2.0. seguridad en la red para la familia*. Editorial Paulinas.

Constitución Española. *Boletín Oficial del Estado, 29 de diciembre de 1978,* 311, 29313-29424.

Domingo, J. (2008). El aprendizaje cooperativo. *Cuadernos de trabajo social*, 21, 231-246.

Egele, M., Kruegel, C., Kirda, E., Yin, H., y Song, D. (17-22 de Junio de 2007). Dynamic spyware analysis. En J. Chase y S. Seshan (Presidencia), *2007 Usenix Annual Technical Conference*. Santa Clara, California, EEUU.

Fajardo, M.I., Gordillo, M., y Regalado, A. B. (2013). Sexting: Nuevos usos de la tecnología y la sexualidad en adolescentes. *International Journal of Developmental and Educational Psychology*, 1(1), 521-533.

Fariñas, J. R. (2011). El Impacto de las Redes Sociales en la Propiedad Intelectual. *Propiedad Intelectual*, X (14), 150-173.

Ficarra, F. (2002). Los virus informaticos. *Chasqui. Revista Latinoamericana de Comunicación*, (78), 62-69.

Galence, V. (2011). El ciber-acoso con intención sexual y el child-grooming. *Quadernos de criminología: revista de criminología y ciencias forenses*, (15), 22-33.

Garaigordobil, M. (2015). Ciberbullying en adolescentes y jóvenes del País Vasco: Cambios con la edad. *Anales de Psicología / Annals of Psychology*, 31(3), 1069-1076. https://doi.org/10.6018/analesps.31.3.179151

Giant, N. (2016). *Ciber seguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones*. Narcea Ediciones.

Herranz, E., y Colomo-Palacios, R. (2012). La Gamificación como agente de cambio en la Ingeniería del Software. *Revista de Procesos y Métricas,* 9(2), 30-56.

Hunicke, R., LeBlanc, M., y Zubek, R. (2004). MDA: A formal approach to game design and game research. *Proceedings of the AAAI Workshop on Challenges in Game AI*, 4(1), 1722-1726.

Instituto Nacional de Estadística. (2020). *Equipamiento y uso de TIC en los hogares*. https://bit.ly/2PFJ9GK

Jakobsson, M. (2005). Modeling and preventing phishing attacks. *Financial Cryptography*, 5, 1-19.

Leiva-Aguilera, J. (2009). *Redes sociales: situación y tendencias en relación a la información y documentación*. Baratz.

Marczewski, A. (2015). *User Types. In Even Ninja Monkeys Like to Play: Gamification, Game Thinking and Motivational Design*. CreateSpace Independent Publishing Platform.

Ministerio de Interior. (2019). *Estudio sobre la Cibercriminalidad en España.* Ministerio de Interior.

O'Gorman, G., y McDonald, G. (2012). *Ransomware: A growing menace*. Symantec Corporation.

Oliva, H. A. (2016). La gamificación como estrategia metodológica en el contexto educativo universitario. *Realidad y Reflexión,* 16(44), 108-118.

Orihuela, J. L. (2008). Internet: la hora de las redes sociales. *Nueva Revista,* 119, 57-62.

Pineda, L. O., Jiménez, S. C. (2020). Amenazas a la privacidad de los menores de edad a partir del sharenting. *Revista Chilena de Derecho y Tecnología*, 9(2), 105-130. https://doi.org/10.5354/0719-2584.2020.55333

Qustodio. (2020). *Lanzamiento del 2020 estudio sobre los hábitos online de menores: Apps y nativos digitales: la nueva normalidad*. https://bit.ly/3e5UqJD

Ripoll, O. (2016). "Taller de creació de jocs", una asignatura gamificada. En R. S. Contreras y J. L. Eguia (Eds.), *Gamificación en las aulas universitarias* (25-38). Institut de la Comunicació, Universidad Autónoma de Barcelona.

Rodríguez, C. Z., Simón, L. F. R. (2020). Piratas y creadores: autoría, creatividad y automatización en Youtube. *Cuadernos de Documentación Multimedia*, 31, 1-8. https://doi.org/10.5209/cdmu.68441

Teixes, F. (2014). *Gamificación: Fundamentos y aplicaciones*. Editorial UOC.

Teixes, F. (2015). *Gamificación: motivar jugando*. Editorial UOC.

Torrego, J. C., y Negro, A. (2014). *Aprendizaje cooperativo en las aulas*. Alianza Editorial.

Torres-Toukoumidis, Á., y Romero-Rodríguez, L. M. (2018). Aprender jugando. La gamificación en el aula. *Educar para los nuevos Medios*, 61-72.

Valderrama, B. (2015). Los secretos de la gamificación: 10 motivos para jugar. *Capital Humano*, 295, 73-78.

Viaña de Avendaño, G. (5-9 de Septiembre de 2016). La importancia de la incorporación de la figura delictiva denominada "grooming". *XVI Simposio Argentino de Informática y Derecho (SID 2016)-JAIIO 45.* Universidad Nacional de Tres de Febrero, Buenos Aires, Argentina.

Wachowski, A., y Wachowski, L. (1999). *The matrix* [Película]. Warner Home Video.

Werbach, K, y Hunter, D. (2012). *For the Win: how Game Thinking Can Revolutionize Your Business*. Wharton Digital Press.

Zichermann, G., y Cunningham, C. (2011). *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*. O'Reilly Media.

Anexo A. Alumnado CEIP San Fernando (2019)

CURSO	TOTAL	ALUMNAS	ALUMNOS
Educación Infantil (3 años)	46	22	24
Infantil A	23	12	11
Infantil B	23	10	13
Educación Infantil (4 años)	50	23	27
Infantil A	24	11	13
Infantil B	26	12	14
Educación Infantil (5 años)	51	27	24
Infantil A	26	16	10
Infantil B	25	11	14
1º Educación Primaria	49	21	28
1ºA	23	9	14
1ºB	24	11	13
2º Educación Primaria	50	16	34
2ºA	25	9	16
2ºB	25	7	18
3ºEducación Primaria	49	23	26
3ºA	23	11	12
3ºB	25	11	14

4º Educación Primaria	50	22	28
4ºA	25	11	14
4ºB	25	11	14
5º Educación Primaria	50	22	28
5ºA	25	11	14
5ºB	25	11	14
6º Educación Primaria	56	25	31
6ºA	19	8	11
6ºB	21	8	13
6ºC	16	9	7
Número de aulas: 19			

Anexo B. Rúbricas

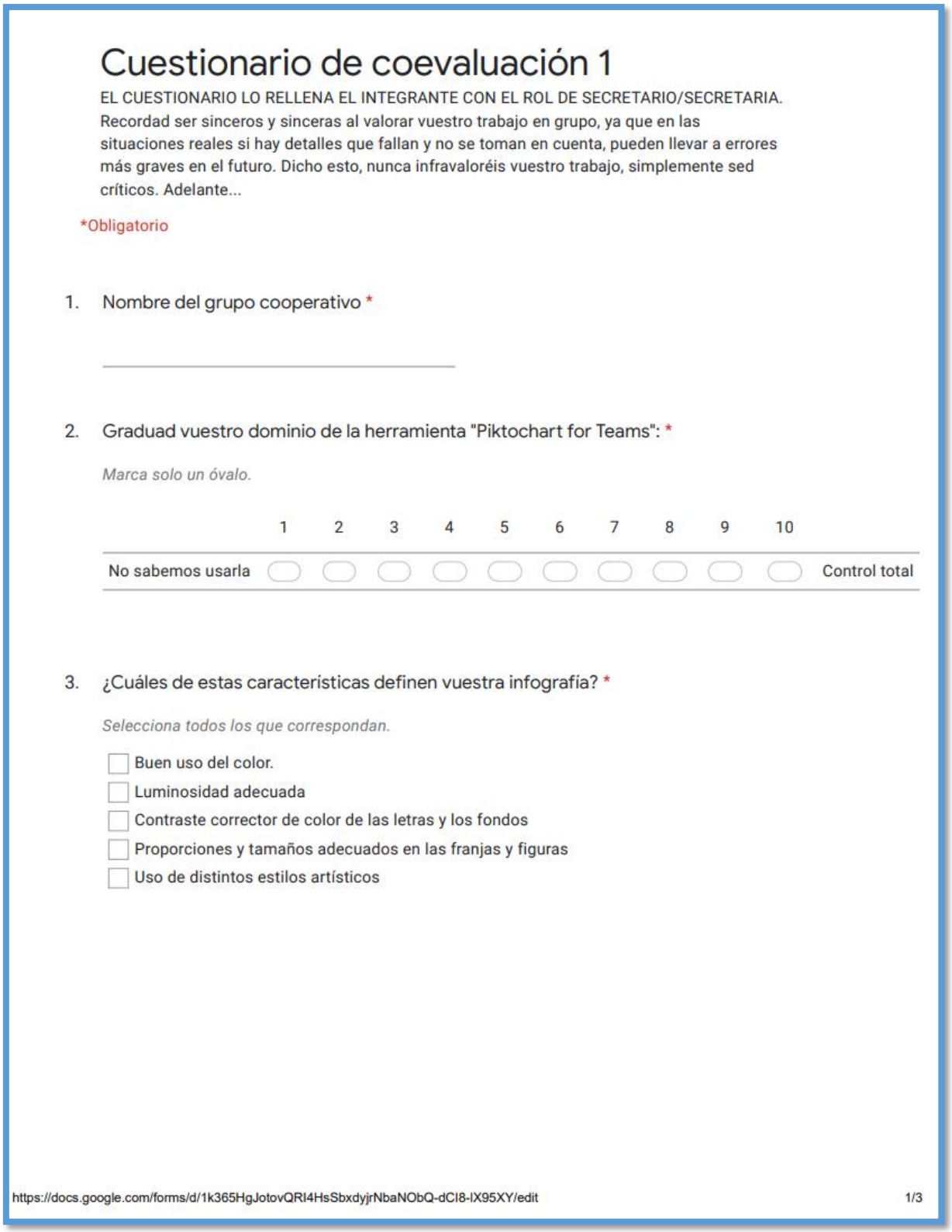
SITUACIÓN DE APRENDIZAJE: "Exploit City"				
RÚBRICA 1 – ACTIVIDAD 3				
Parámetros para evaluar	**Insuficiente (0,83 puntos)**	**Suficiente (1,66 puntos)**	**Notable (2,49 puntos)**	**Sobresaliente (3,33 puntos)**
Citación	La norma para las citas no se usa en ningún momento.	La norma para las citas se emplea, aunque con omisiones de ciertos campos.	La norma para las citas se emplea de forma eficiente en la mayoría de las ocasiones.	La norma para las citas se usa de forma óptima en todo momento, independientemente de la fuente.
Coherencia textual	El texto está compuesto por ideas no entrelazadas.	El texto contiene ciertas ideas correctamente enlazadas, aunque sin emplear nexos.	El texto está formado, en su mayoría, por ideas conectadas, haciendo además un uso adecuado de los nexos.	El texto está perfectamente ideado en términos de coherencia, haciendo uso de nexos y conectores para conectar las frases.
Ortografía	Las oraciones contienen muchos errores de ortografía o puntuación.	Las oraciones contienen errores de ortografía o puntuación en varias ocasiones.	Las oraciones contienen errores de ortografía o puntuación en momentos extremadamente puntuales.	Las oraciones no contienen errores de ortografía o puntuación, exceptuando alguna situación desconocida lingüísticamente.
Estándares de aprendizaje evaluables relacionados: 30, 61, 64, 72, 73 (LCL) - 14, 16 (CS)				

SITUACIÓN DE APRENDIZAJE: "Exploit City"				
RÚBRICA 2 – ACTIVIDAD 6				
Parámetros para evaluar	**Insuficiente (0,83 puntos)**	**Suficiente (1,66 puntos)**	**Notable (2,49 puntos)**	**Sobresaliente (3,33 puntos)**
Trabajo cooperativo	Los roles y funciones en el grupo se evitan, complicando el trabajo en todos los niveles.	Los roles y funciones en el grupo se cumplen, aunque han existido complicaciones puntuales sin mediación.	Los roles y funciones en el grupo se cumplen, aunque han existido complicaciones que, por suerte, se han solucionado con mediación.	Los roles y funciones en el grupo se cumplen eficazmente, además sin afrontar problemas de trabajo, lo cual ha facilitado el alcance de un mejor producto.
Diseño artístico	Las características del color y sus propiedades se emplean de forma irregular.	Las características del color y sus propiedades se emplean de forma lógica, pero sin una pauta general.	Las características del color y sus propiedades se combinan coherentemente, exceptuando algún apartado cromático.	Las características del color y sus propiedades se combinan obteniendo la mejor expresión posible de la producción artística, demostrando un gran dominio.
Ortografía	Las oraciones contienen muchos errores de ortografía o puntuación, a pesar de usar corrector digital.	Las oraciones contienen errores de ortografía o puntuación en varias ocasiones, a pesar de usar corrector digital.	Las oraciones contienen errores de ortografía o puntuación en momentos extremadamente puntuales, usando bien el corrector.	Las oraciones no contienen errores de ortografía o puntuación, exceptuando alguna situación desconocida lingüísticamente, demostrando un buen uso de las herramientas digitales.
Estándares de aprendizaje evaluables relacionados: 60, 61, 75, 76 (LCL) - 11, 17 (CS) - 14, 18, 20 (EA)				

SITUACIÓN DE APRENDIZAJE: "Exploit City"				
RÚBRICA 3 – ACTIVIDAD 9				
Parámetros para evaluar	**Insuficiente (1,25 puntos)**	**Suficiente (2,50 puntos)**	**Notable (3,75 puntos)**	**Sobresaliente (5,00 puntos)**
Diseño artístico	Las características del color y sus propiedades se emplean de forma irregular.	Las características del color y sus propiedades se emplean de forma lógica, pero sin una pauta general.	Las características del color y sus propiedades se combinan coherentemente, exceptuando algún apartado cromático.	Las características del color y sus propiedades se combinan obteniendo la mejor expresión posible de la producción artística, demostrando un gran dominio.
Ortografía	Las oraciones contienen muchos errores de ortografía o puntuación, a pesar de usar corrector digital.	Las oraciones contienen errores de ortografía o puntuación en varias ocasiones, a pesar de usar corrector digital.	Las oraciones contienen errores de ortografía o puntuación en momentos extremadamente puntuales, usando bien el corrector.	Las oraciones no contienen errores de ortografía o puntuación, exceptuando alguna situación desconocida lingüísticamente, demostrando un buen uso de las herramientas digitales.
Estándares de aprendizaje evaluables relacionados: 60, 64, 76 (LCL) - 14, 18, 20 (EA)				

SITUACIÓN DE APRENDIZAJE: "Exploit City"				
RÚBRICA 4 – ACTIVIDAD 12				
Parámetros para evaluar	**Insuficiente (1,25 puntos)**	**Suficiente (2,50 puntos)**	**Notable (3,75 puntos)**	**Sobresaliente (5,00 puntos)**
Lenguaje artístico	Los elementos visuales transmiten un mensaje o erróneo de forma evidente, favoreciendo una difusión equívoca.	Los elementos visuales transmiten un mensaje acertado, pero algunos elementos no cumplen su función, favoreciendo una difusión muy interpretable.	Los elementos visuales transmiten un mensaje acertado, logrando difundir una idea cercana a la representada en la producción.	Los elementos visuales transmiten un mensaje acertado, logrando difundir una idea exacta o muy vinculada con la que se buscaba representar en la producción.
Diseño artístico	Las características del color y sus propiedades se emplean de forma irregular.	Las características del color y sus propiedades se emplean de forma lógica, pero sin una pauta general.	Las características del color y sus propiedades se combinan coherentemente, exceptuando algún apartado cromático.	Las características del color y sus propiedades se combinan obteniendo la mejor expresión posible de la producción artística, demostrando un gran dominio.
Estándares de aprendizaje evaluables relacionados: • 6, 10, 12, 14, 18, 20 (EA)				

Anexo C. Cuestionarios de coevaluación



Cuestionario de coevaluación 1

EL CUESTIONARIO LO RELLENA EL INTEGRANTE CON EL ROL DE SECRETARIO/SECRETARIA. Recordad ser sinceros y sinceras al valorar vuestro trabajo en grupo, ya que en las situaciones reales si hay detalles que fallan y no se toman en cuenta, pueden llevar a errores más graves en el futuro. Dicho esto, nunca infravaloréis vuestro trabajo, simplemente sed críticos. Adelante...

*Obligatorio

1. Nombre del grupo cooperativo *

2. Graduad vuestro dominio de la herramienta "Piktochart for Teams": *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
No sabemos usarla											Control total

3. ¿Cuáles de estas características definen vuestra infografía? *

Selecciona todos los que correspondan.

- [ ] Buen uso del color.
- [ ] Luminosidad adecuada
- [ ] Contraste corrector de color de las letras y los fondos
- [ ] Proporciones y tamaños adecuados en las franjas y figuras
- [ ] Uso de distintos estilos artísticos

https://docs.google.com/forms/d/1k365HgJotovQRI4HsSbxdyjrNbaNObQ-dCI8-IX95XY/edit 1/3

4. Decid la licencia escogida para vuestra infografía y explicad por qué es la mejor para el caso que os tocó en la tarjeta: *

5. ¿Qué nivel de importancia tiene para vuestro grupo que os den el reconocimiento por vuestra obra? *

Marca solo un óvalo.

	1	2	3	4	5	
Poco	◯	◯	◯	◯	◯	Mucho

6. ¿Qué nivel de importancia da vuestro grupo a que se pueda usar vuestra obra para fines que no podéis controlar? *

Marca solo un óvalo.

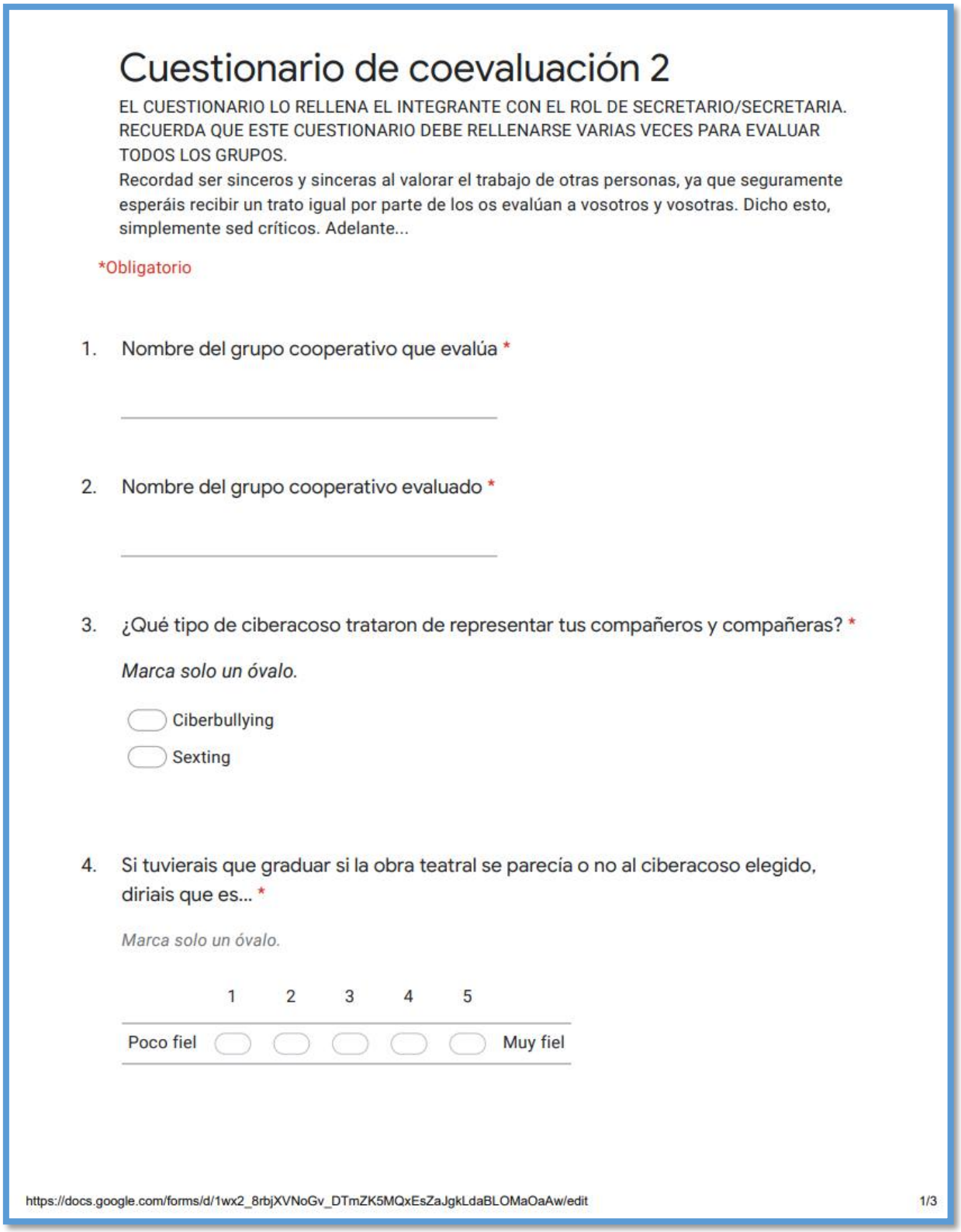
	1	2	3	4	5	
Poco	◯	◯	◯	◯	◯	Mucho

7. Para último, indicad la calificación que os daríais en la actividad (sed sinceros y sinceras): *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Mal	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Excelente

https://docs.google.com/forms/d/1k365HgJotovQRI4HsSbxdyjrNbaNObQ-dCI8-IX95XY/edit 2/3



Cuestionario de coevaluación 2

EL CUESTIONARIO LO RELLENA EL INTEGRANTE CON EL ROL DE SECRETARIO/SECRETARIA. RECUERDA QUE ESTE CUESTIONARIO DEBE RELLENARSE VARIAS VECES PARA EVALUAR TODOS LOS GRUPOS.
Recordad ser sinceros y sinceras al valorar el trabajo de otras personas, ya que seguramente esperáis recibir un trato igual por parte de los os evalúan a vosotros y vosotras. Dicho esto, simplemente sed críticos. Adelante...

*Obligatorio

1. Nombre del grupo cooperativo que evalúa *

2. Nombre del grupo cooperativo evaluado *

3. ¿Qué tipo de ciberacoso trataron de representar tus compañeros y compañeras? *

Marca solo un óvalo.

- Ciberbullying
- Sexting

4. Si tuvierais que graduar si la obra teatral se parecía o no al ciberacoso elegido, diriais que es... *

Marca solo un óvalo.

	1	2	3	4	5	
Poco fiel						Muy fiel

https://docs.google.com/forms/d/1wx2_8rbjXVNoGv_DTmZK5MQxEsZaJgkLdaBLOMaOaAw/edit 1/3

5. ¿Consideráis que los compañeros y compañeras se sabían bien su guion? *

Marca solo un óvalo.

- ◯ Sí, al completo.
- ◯ No, leyeron demasiado.
- ◯ Parcialmente, hubo partes mejores y otras peores.
- ◯ No sabemos que contestar.

6. ¿Consideráis que el decorado y el vestuario fueron adecuados para la obra representada? *

Marca solo un óvalo.

- ◯ Sí, nos ayudaron a vernos inmersos en la obra.
- ◯ No, hubieron muchos detalles que no se ajustaban a la obra.
- ◯ En general, estuvo bien, más allá de que hubiera o no ciertos defectos.
- ◯ No sabemos que contestar.

7. ¿Creéis que el debate posterior a la obra fue bien conducido por el grupo que exponía la obra? *

Marca solo un óvalo.

- ◯ Sí, plantearon posibles soluciones y cuestiones que nos ayudaron a reflexionar el caso.
- ◯ No, plantearon cuestiones que no tenían nada que ver con su situación de ciberacoso.
- ◯ No estuvo mal, hubieron ciertos aspectos que podrían ayudar a solucionar el caso.
- ◯ No sabemos que contestar.

8. Si tuvierais que calificar la calidad de la obra de los compañeros y compañeras tendría una calificación de... *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Mal	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Excelente

Este contenido no ha sido creado ni aprobado por Google.

Google Formularios

https://docs.google.com/forms/d/1wx2_8rbjXVNoGv_DTmZK5MQxEsZaJgkLdaBLOMaOaAw/edit 3/3

Cuestionario de coevaluación 3

Familias: En el apartado de nombre del grupo que evalúa escribid "Familia de NOMBRE DE VUESTRO HIJO O HIJA (poner apellido en caso de repetición)". Responded a las distintas preguntas con la máxima sinceridad. Disfrutad de las presentaciones, traerán un tema que nos interesa a todos por nuestra seguridad en la red.

Alumnado: EL CUESTIONARIO LO RELLENA EL INTEGRANTE CON EL ROL DE SECRETARIO/SECRETARIA. RECUERDA QUE ESTE CUESTIONARIO DEBE RELLENARSE VARIAS VECES PARA EVALUAR TODOS LOS GRUPOS.
Recordad ser sinceros y sinceras al valorar el trabajo de otras personas, ya que seguramente esperáis recibir un trato igual por parte de los os evalúan a vosotros y vosotras. Dicho esto, simplemente sed críticos. Adelante...

*Obligatorio

1. Nombre del grupo que evalúa *

2. Nombre del grupo evaluado *

3. Tras escuchar la presentación del virus, señala qué detalles habéis entendido (marca una o más): *

Selecciona todos los que correspondan.

- [ ] Somos capaces de describir con nuestras palabras el programa maligno o virus.
- [ ] Somos capaces de detallar de forma básica el funcionamiento y procesos del virus.
- [ ] Somos capaces de recordar algún caso de los ataques comentados, o de recordar algún otro similar.
- [ ] Somos capaces de usar o aplicar algunos métodos de defensa de los comentados.
- [ ] La presentación ha sido confusa (por cualquier motivo de comunicación, información o diseño) y no hemos entendido nada.

https://docs.google.com/forms/d/1Pa-IMEVBCHEPF-BE9Vqos7OoeQkhOsP7Z7jrEWc3Pbg/edit 1/3

4. La presentación ha permitido participar comunicativamente a: *

Marca solo un óvalo.

- ◯ todos los integrantes.
- ◯ todos los integrantes, con cierta desigualdad en los tiempos.
- ◯ algunos integrantes, quedando otros sin hablar o sin apenas participar.

5. Si analizamos los aspectos orales, podemos decir que: *

Marca solo un óvalo por fila.

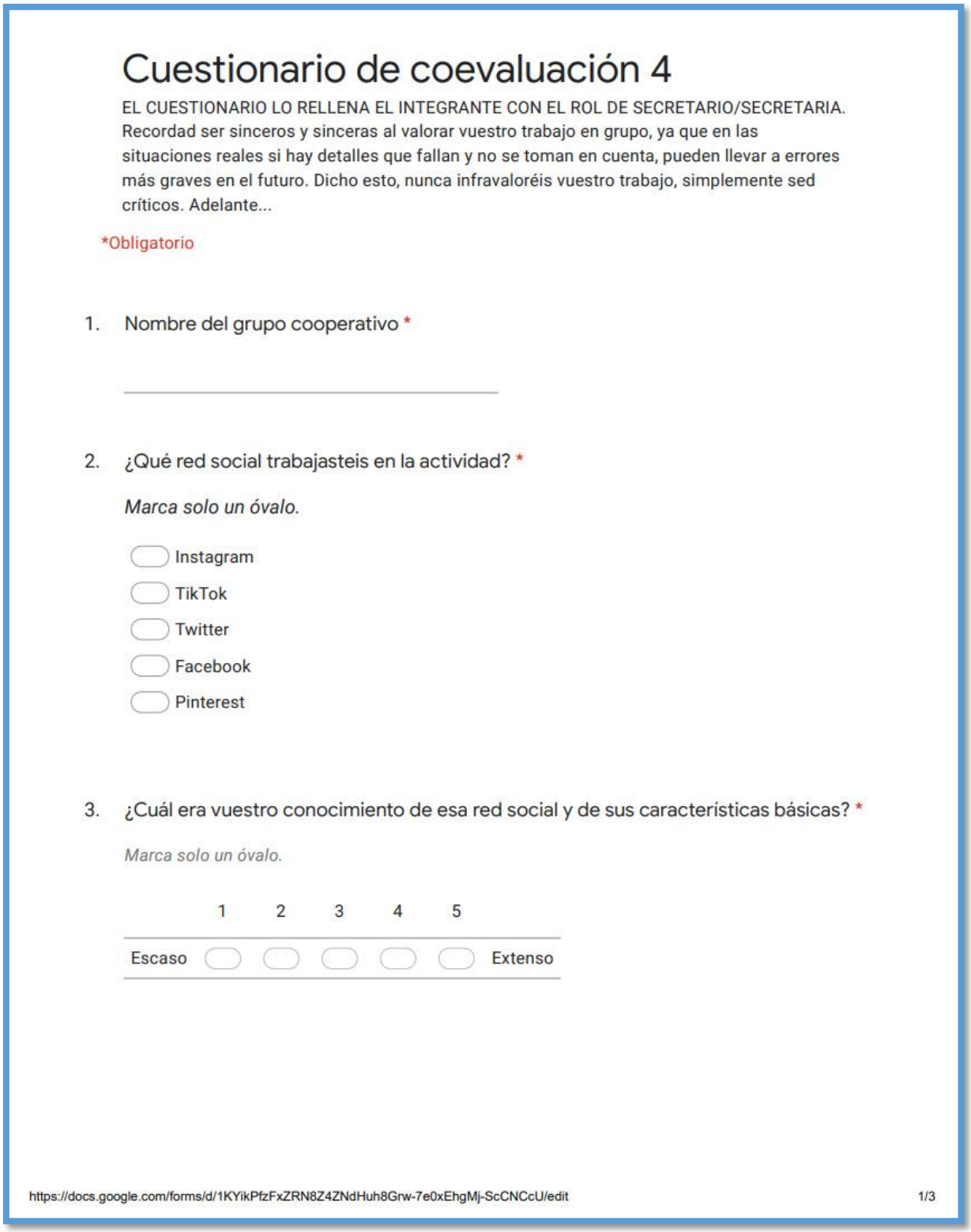
	Excelente	Bien	Suficiente	Mal	Ns/Nc
Entonación	◯	◯	◯	◯	◯
Lenguaje corporal	◯	◯	◯	◯	◯
Volumen	◯	◯	◯	◯	◯
Ritmo	◯	◯	◯	◯	◯
Claridad	◯	◯	◯	◯	◯

6. ¿Qué detalles podrían haberse incluido o mejorado para hacer una presentación todavía mejor? (No hace falta extenderse, es suficiente con mencionarlos) *

7. Si tuvierais que calificar la calidad de la presentación tendría una calificación de... *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Mal	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Excelente



Cuestionario de coevaluación 4

EL CUESTIONARIO LO RELLENA EL INTEGRANTE CON EL ROL DE SECRETARIO/SECRETARIA. Recordad ser sinceros y sinceras al valorar vuestro trabajo en grupo, ya que en las situaciones reales si hay detalles que fallan y no se toman en cuenta, pueden llevar a errores más graves en el futuro. Dicho esto, nunca infravaloréis vuestro trabajo, simplemente sed críticos. Adelante...

*Obligatorio

1. Nombre del grupo cooperativo *

2. ¿Qué red social trabajasteis en la actividad? *

Marca solo un óvalo.

- Instagram
- TikTok
- Twitter
- Facebook
- Pinterest

3. ¿Cuál era vuestro conocimiento de esa red social y de sus características básicas? *

Marca solo un óvalo.

	1	2	3	4	5	
Escaso						Extenso

https://docs.google.com/forms/d/1KYikPfzFxZRN8Z4ZNdHuh8Grw-7e0xEhgMj-ScCNCcU/edit 1/3

4. Tras haber finalizado la actividad, ¿consideráis que sois capaces de emplear correctamente todas las funciones de dicha red social? *

Marca solo un óvalo.

- ◯ Posiblemente podemos usar la mayoría y nos hemos familiarizado bien con la configuración.
- ◯ Podemos usar una cantidad razonable de opciones, pero quizás algunos detalles se nos han escapado.
- ◯ No exploramos suficientemente las opciones, hemos tenido percances o problemas.

5. ¿Qué tipo de técnicas habéis usado para promocionar el evento "Redundancia" en vuestra red social? *

Selecciona todos los que correspondan.

- ☐ Eslogan.
- ☐ Asistente modelo (perfil del evento).
- ☐ Simpatía en la red (poner bromas, memes, gifs relacionados...).
- ☐ Anuncios publicitarios.

6. ¿Cuál de las técnicas publicitarias utilizadas os parece la más efectiva? Explicad por qué. *

7. ¿Qué dominio y conocimiento tenéis del uso del apartado de configuración de la red social? *

Marca solo un óvalo.

	1	2	3	4	5	
Escaso	◯	◯	◯	◯	◯	Extenso

8. ¿Qué opción os ha parecido la más útil para restringir la privacidad del perfil? *

_____

9. Para último, indicad la calificación que os daríais en la actividad (sed sinceros y sinceras): *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Mal	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Excelente

Cuestionario de coevaluación 5

RECORDAD QUE TENÉIS QUE HABER ENTREGADO EL INFORME CON TODAS LAS OPERACIONES Y PROBLEMAS DE CADA INTEGRANTE DEL GRUPO (TODO JUNTO) PARA PODER REALIZAR EL CUESTIONARIO. EL CUESTIONARIO LO RELLENA EL INTEGRANTE CON EL ROL DE SECRETARIO/SECRETARIA.

Recordad ser sinceros y sinceras al valorar vuestro trabajo en grupo, ya que en las situaciones reales si hay detalles que fallan y no se toman en cuenta, pueden llevar a errores más graves en el futuro. Dicho esto, nunca infravaloréis vuestro trabajo, simplemente sed críticos. Adelante...

*Obligatorio

1. Nombre del grupo cooperativo *

_____

2. En todo momento todos los integrantes hemos realizado las operaciones y problemas por nuestra cuenta, aunque luego pudiéramos ayudarnos en las correcciones. *

Marca solo un óvalo.

- ◯ Sí.
- ◯ No.
- ◯ En ocasiones hemos dejado operaciones sin hacer.

3. ¿En qué tipo de operaciones y problemas ha tenido más dificultades el grupo? (Pueden marcarse varias) *

Selecciona todos los que correspondan.

- ☐ Potencias
- ☐ Fracciones
- ☐ Operaciones combinadas (Jerarquía de operaciones)
- ☐ Porcentajes (regla de 3 y cálculo de los mismos)

https://docs.google.com/forms/d/1qkiddw_5y7o6uXkB7t1KvnKsQFwfR2wYcUXlHRB0RGg/edit 1/3

4. ¿Qué tipo de ayudas se han dado a los integrantes que tenían dificultades en alguna ocasión? *

Selecciona todos los que correspondan.

- [ ] Explicación detallada del proceso de resolución.
- [ ] Correcciones leves en el cálculo.
- [ ] Lectura pausada del enunciado del problema en grupo.
- [ ] Plantear esquemas, diagramas partes-todo u otros elementos gráficos visuales.
- [ ] Resolver hacia atrás el problema u operación como explicación.

5. *

Marca solo un óvalo por fila.

	Superadas por todo el grupo	No superadas por ningún miembro	Existen uno o más integrantes con problemas
Cálculo de operaciones (suma y resta)	◯	◯	◯
Cálculo de operaciones (multiplicación y división)	◯	◯	◯
Operaciones con fracciones	◯	◯	◯
Cálculo de M.C.M y M.C.D	◯	◯	◯
Potencias	◯	◯	◯
Operaciones con potencias	◯	◯	◯
Jerarquía de operaciones (orden)	◯	◯	◯
Porcentajes y su cálculo	◯	◯	◯
Regla de 3	◯	◯	◯

https://docs.google.com/forms/d/1qkiddw_5y7o6uXkB7t1KvnKsQFwfR2wYcUXlHRB0RGg/edit 2/3

6. ¿Qué proceso se seguía en la resolución de problemas? *

Marca solo un óvalo.

- 1 - Lectura del enunciado, 2 - Detectar datos, relaciones y objetivos del problema, 3 - Realizar diagrama partes - todo o esquema gráfico, 4 - Elegir una estrategia de resolución y ejecutarla, 5 - Dar la solución y comprobarla resolviendo hacia atrás el problema
- 1 - Lectura del enunciado, 2 - Detectar datos, relaciones y objetivos del problema, 3 - Realizar diagrama partes - todo o esquema gráfico, 4 - Elegir una estrategia de resolución y ejecutarla, 5 - Dar la solución
- 1 - Lectura del enunciado, 2 - Detectar datos, relaciones y objetivos del problema, 3 - Elegir una estrategia de resolución y ejecutarla, 4 - Dar la solución
- Ningún proceso.

7. Para finalizar, aunque hayáis hecho vuestras operaciones siempre por separado, habéis tenido que aseguraros de que todos y todas llegáis al objetivo de tener todas las operaciones y problemas hechos y corregidos (ayudando siempre a avanzar en las dificultades). Por tanto, la responsabilidad es grupal, y la nota será grupal (sed sinceros y sinceras)... *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Mal											Excelente

Anexo D. Formulario de Autoevaluación

Formulario de Autoevaluación

Recuerda ser sincero o sincera al valorar tu propio trabajo, ya que solo la autocrítica puede hacerte mejorar y superarte continuamente. Dicho esto, si tu desempeño te ha permitido mejorar y superar errores, nunca descartes poner una nota perfecta. Adelante...

*Obligatorio

1. Nombre del alumno o alumna: *

2. ¿Qué valor darías a tu conocimiento previo de los contenidos o conceptos que has trabajado? *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Nunca lo había trabajado	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Lo he trabajado en muchas ocasiones

3. ¿En qué nivel situarías tu disposición a la hora de hacer la actividad? *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Muy escasa	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Muy elevada

4. ¿Qué detalles, conceptos o procedimientos de la actividad te han resultado más complejos de aprender? *

5. ¿Podrías especificar dos o tres momentos en los que has cometido algún error? (El objetivo de esta pregunta es la mejora futura de errores)

https://docs.google.com/forms/d/1pr9B_xv7cr1UP2sbFwCvYfuxT9my6kmbfreFxTH7blA/edit 1/2

6. Especifica que habilidades o destrezas has tenido que usar en la actividad (marca las usadas): *

Selecciona todos los que correspondan.

- [ ] Resolución de problemas
- [ ] Trabajar en equipo
- [ ] Comprensión lectora
- [ ] Análisis crítico
- [ ] Análisis experimental
- [ ] Uso de herramientas digitales

7. Indica de forma breve cómo has mejorado una de las habilidades que has señalado:

_____

8. Imagina que no has hecho esta actividad todavia...¿Qué recomendarías a tu "yo" para alcanzar el éxito pleno en esta actividad? *

_____

_____

_____

_____

_____

9. Por último, indica la nota que te darías en esta actividad (recuerda ser sincero o sincera contigo mismo o misma): *

Marca solo un óvalo.

	1	2	3	4	5	6	7	8	9	10	
Mal	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Excelente

Anexo E. Recursos didácticos de las actividades

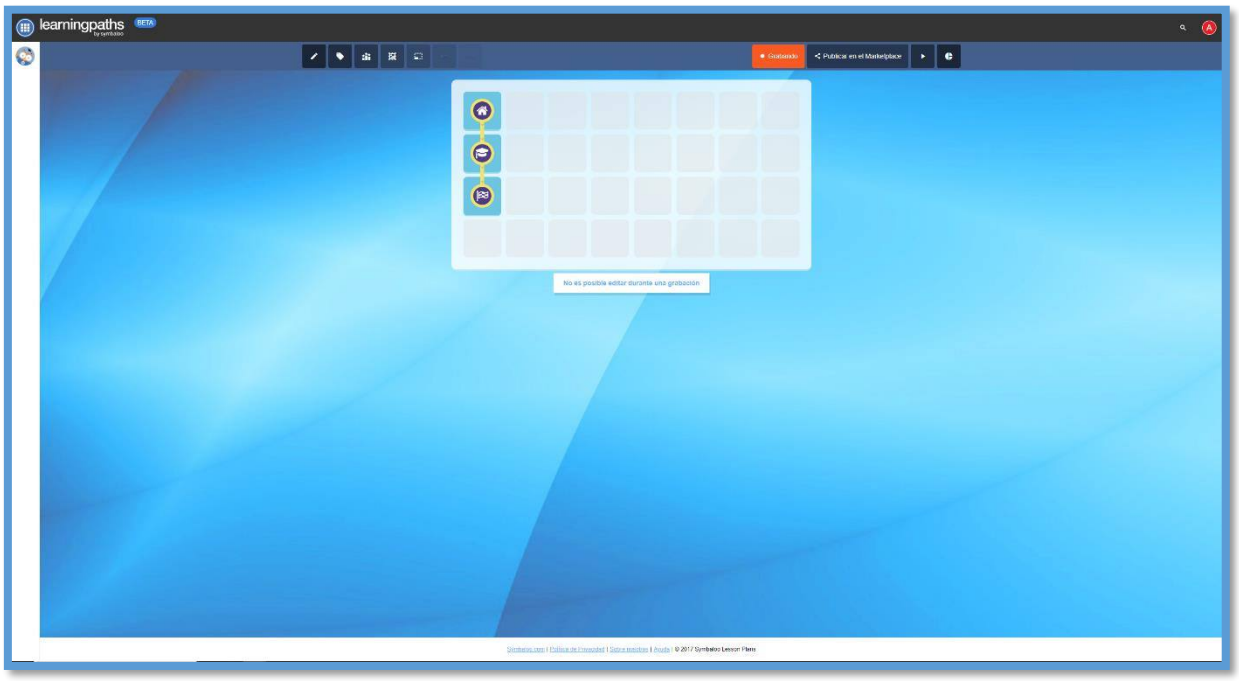
Lista completa de todos los recursos, indicando todos los recursos únicos y originales y su región localizada de descarga o de visionado (solo se incluye enlaces de los propios, ya que el resto son aplicaciones o materiales de tipo tecnológico o escolar). Por otro lado, es importante comentar que todos los creados por el autor tienen su correspondiente licencia Creative Commons (BY – NC – SA 4.0).

- **Recurso 1:** 25 portátiles
- **Recurso 2 (Anexo F):** Symbaloo Lesson Plan (Recurso creado para actividad 1) - Enlace
- **Recurso 3 (Anexo F):** Edpuzzle - Enlace
- **Recurso 4**: Goconqr
- **Recurso 5 (Anexo F):** Documento de casos - Descarga
- **Recurso 6:** Google Drive
- **Recurso 7 (Anexo F):** Vídeo 1 (Recurso creado para actividad 1) - Enlace
- **Recurso 8 (Anexo F):** Vídeo 2 (Recurso creado para actividad 1) - Enlace
- **Recurso 9 (Anexo F)**: Vídeo 3 (Recurso creado para actividad 1) - Enlace
- **Recurso 10:** Piktochart
- **Recurso 11 (Anexo G):** Tarjetas (Recurso creado para actividad 2) - Descarga
- **Recurso 12:** Google Scholar
- **Recurso 13 (Anexo H)**: Guía (Recurso creado para actividad 3) - Descarga
- **Recurso 14 (Anexo I):** Fichas de cuestiones con conversaciones de WhatsApp simuladas (Recurso creado para actividad 4) - Descarga
- **Recurso 15:** Vestuario
- **Recurso 16:** Cartón
- **Recurso 17:** Móviles del alumnado
- **Recurso 18**: Teamviewer
- **Recurso 19:** Canva
- **Recurso 20:** Issuu
- **Recurso 21:** Genial.ly
- **Recurso 22 (Anexo J):** Ficha de trabajo (Recurso creado para actividad 8) - Descarga
- **Recurso 23 (Anexo J):** Virus troyanos (Recurso creado para actividad 8) - Descarga

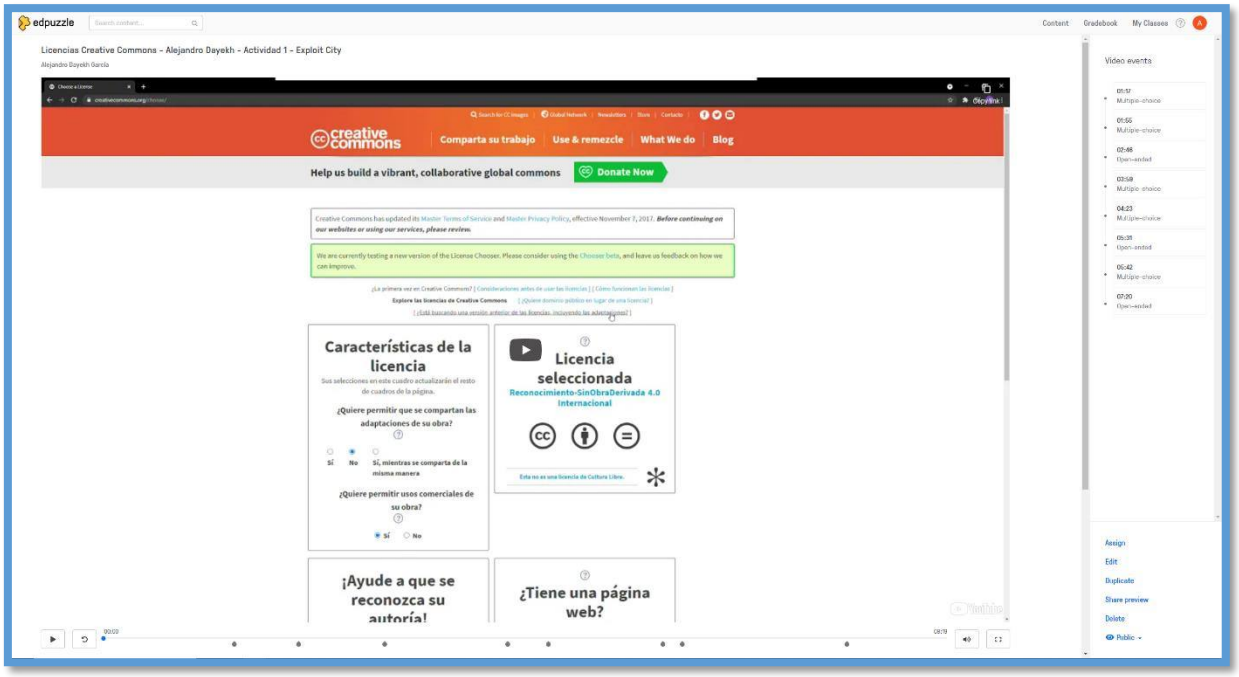
- **Recurso 24 (Anexo J)**: Ficheros de los virus (Recurso creado para actividad 8) - Descarga
- **Recurso 25:** Google Sites
- **Recurso 26:** Condiciones de uso de Twitter
- **Recurso 27:** Condiciones de uso de TikTok
- **Recurso 28**: Condiciones de uso de Pinterest
- **Recurso 29:** Condiciones de uso de Instagram
- **Recurso 30:** Condiciones de uso de Facebook
- **Recurso 31 (Anexo K):** Ficha de cuestiones (Recurso creado para actividad 10) - Descarga
- **Recurso 32:** Cuenta e-mail
- **Recurso 33 (Anexo L):** Instrucciones del grupo Twitter (Recurso creado para actividad 11) -Descarga
- **Recurso 34 (Anexo L)**: Instrucciones del grupo TikTok (Recurso creado para actividad 11) - Descarga
- **Recurso 35 (Anexo L):** Instrucciones del grupo Pinterest (Recurso creado para actividad 11) - Descarga
- **Recurso 36 (Anexo L):** Instrucciones del grupo Instagram (Recurso creado para actividad 11) - Descarga
- **Recurso 37 (Anexo L):** Instrucciones del grupo Facebook (Recurso creado para actividad 11) - Descarga
- **Recurso 38:** Dados de rol del grupo
- **Recurso 39 (Anexo M):** Banco de operaciones y problemas (Recurso creado para actividad 13) - Descarga
- **Justificación legal de uso de RRSS (Anexo N).**

Anexo F. Capturas de recursos de la actividad 1

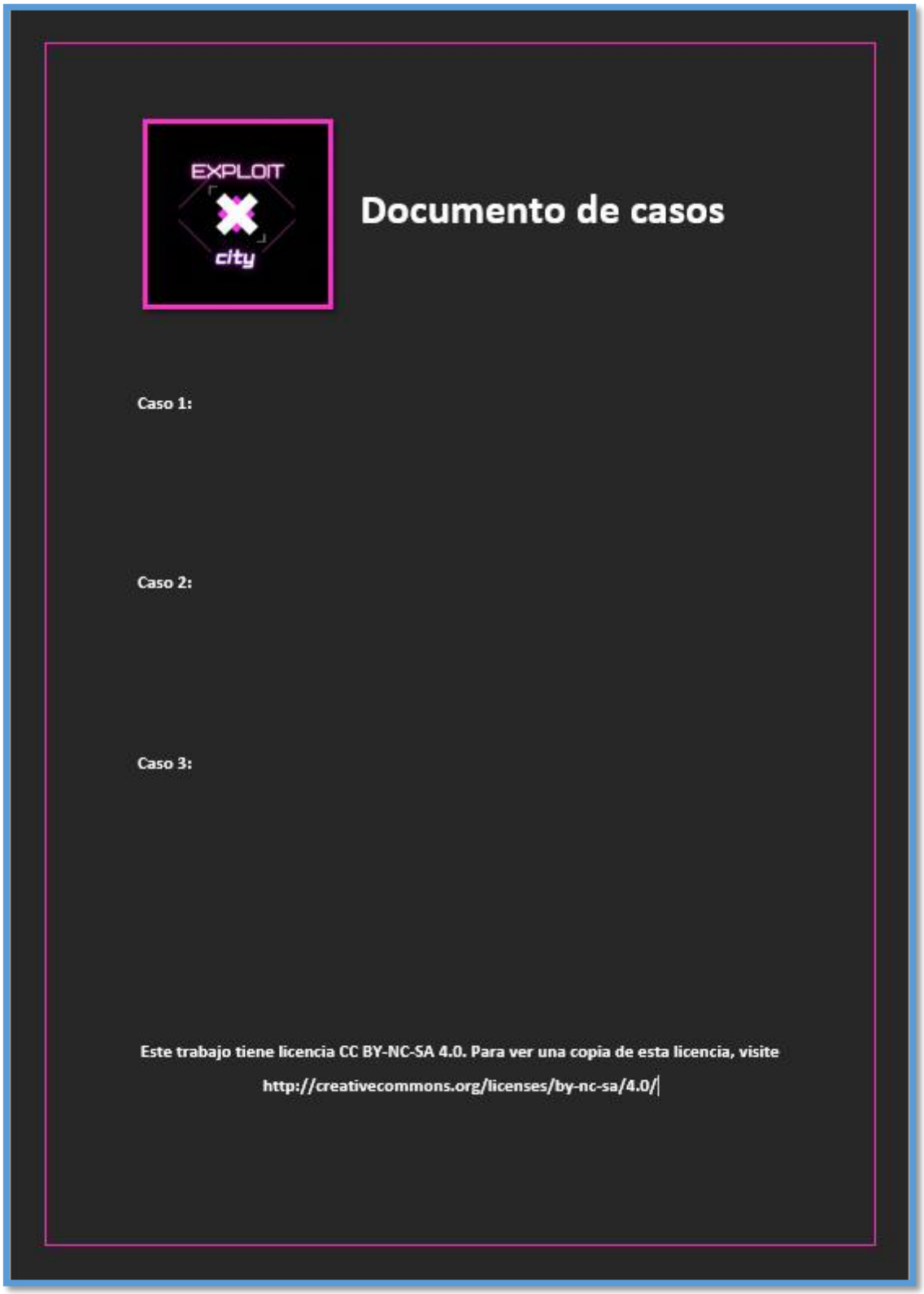
Recurso 2: Symbaloo



Recurso 3: Edpuzzle



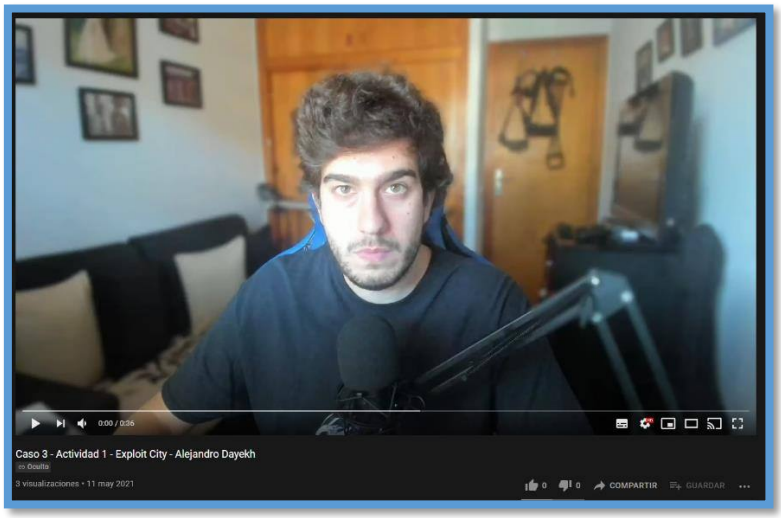
Recurso 5: Documento de casos



Recurso 7: Vídeo 1

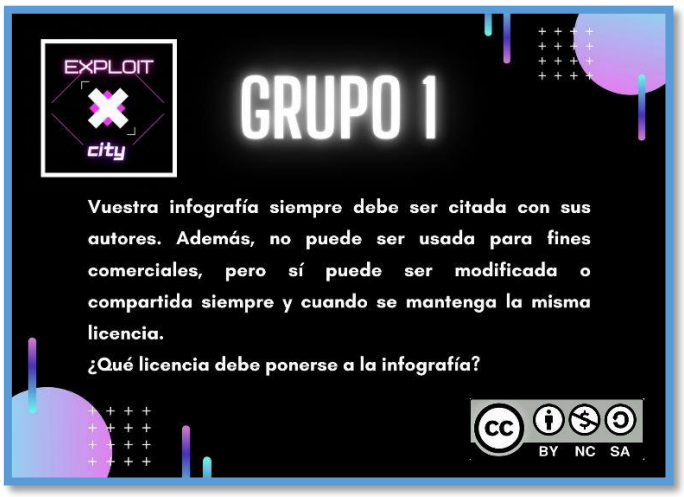
Recurso 8: Vídeo 2

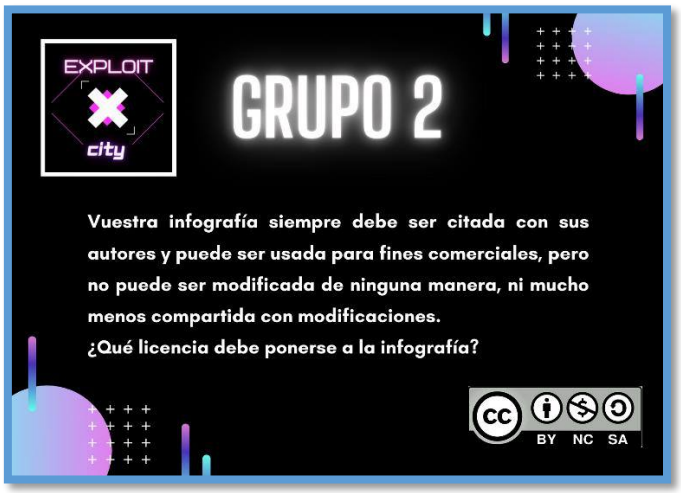
Recurso 9: Vídeo 3



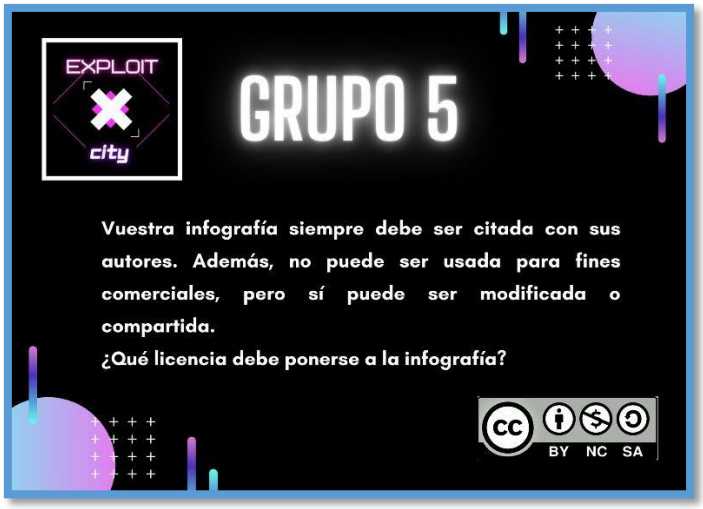
Anexo G. Capturas de recursos de la actividad 2

Recurso 11: Tarjetas



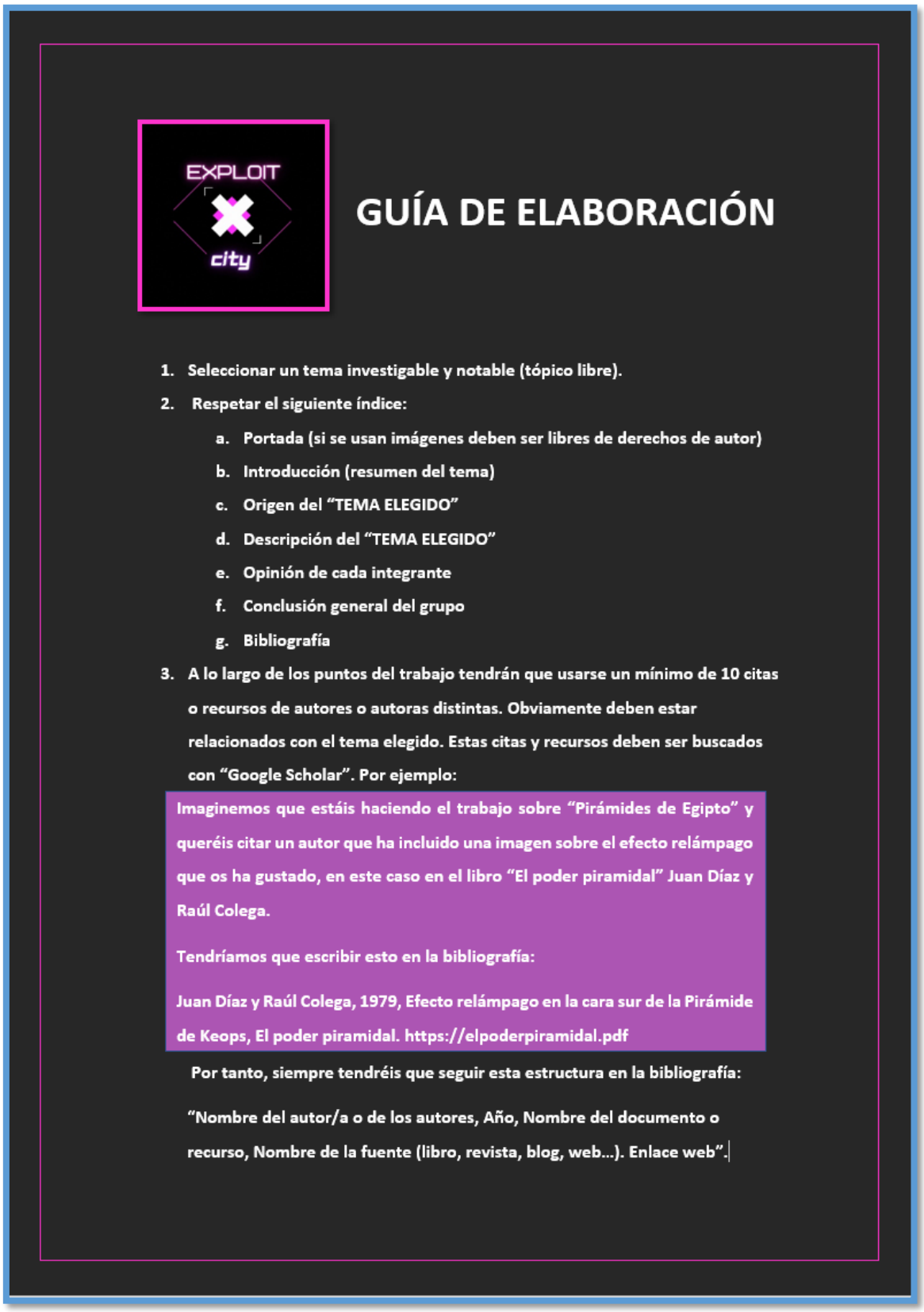



EXPLOIT
city
GRUPO 4
Vuestra infografía puede ser modificada, empleada comercialmente, compartida...El único requisito es que debe darse el reconocimiento a sus creadores.
¿Qué licencia debe ponerse a la infografía?
BY NC SA


EXPLOIT
city
GRUPO 5
Vuestra infografía siempre debe ser citada con sus autores. Además, no puede ser usada para fines comerciales, pero sí puede ser modificada o compartida.
¿Qué licencia debe ponerse a la infografía?
BY NC SA

Anexo H. Capturas de recursos de la actividad 3

Recurso 13: Guía de elaboración



EXPLOIT city

GUÍA DE ELABORACIÓN

1. Seleccionar un tema investigable y notable (tópico libre).
2. Respetar el siguiente índice:
   a. Portada (si se usan imágenes deben ser libres de derechos de autor)
   b. Introducción (resumen del tema)
   c. Origen del "TEMA ELEGIDO"
   d. Descripción del "TEMA ELEGIDO"
   e. Opinión de cada integrante
   f. Conclusión general del grupo
   g. Bibliografía
3. A lo largo de los puntos del trabajo tendrán que usarse un mínimo de 10 citas o recursos de autores o autoras distintas. Obviamente deben estar relacionados con el tema elegido. Estas citas y recursos deben ser buscados con "Google Scholar". Por ejemplo:

Imaginemos que estáis haciendo el trabajo sobre "Pirámides de Egipto" y queréis citar un autor que ha incluido una imagen sobre el efecto relámpago que os ha gustado, en este caso en el libro "El poder piramidal" Juan Díaz y Raúl Colega.

Tendríamos que escribir esto en la bibliografía:

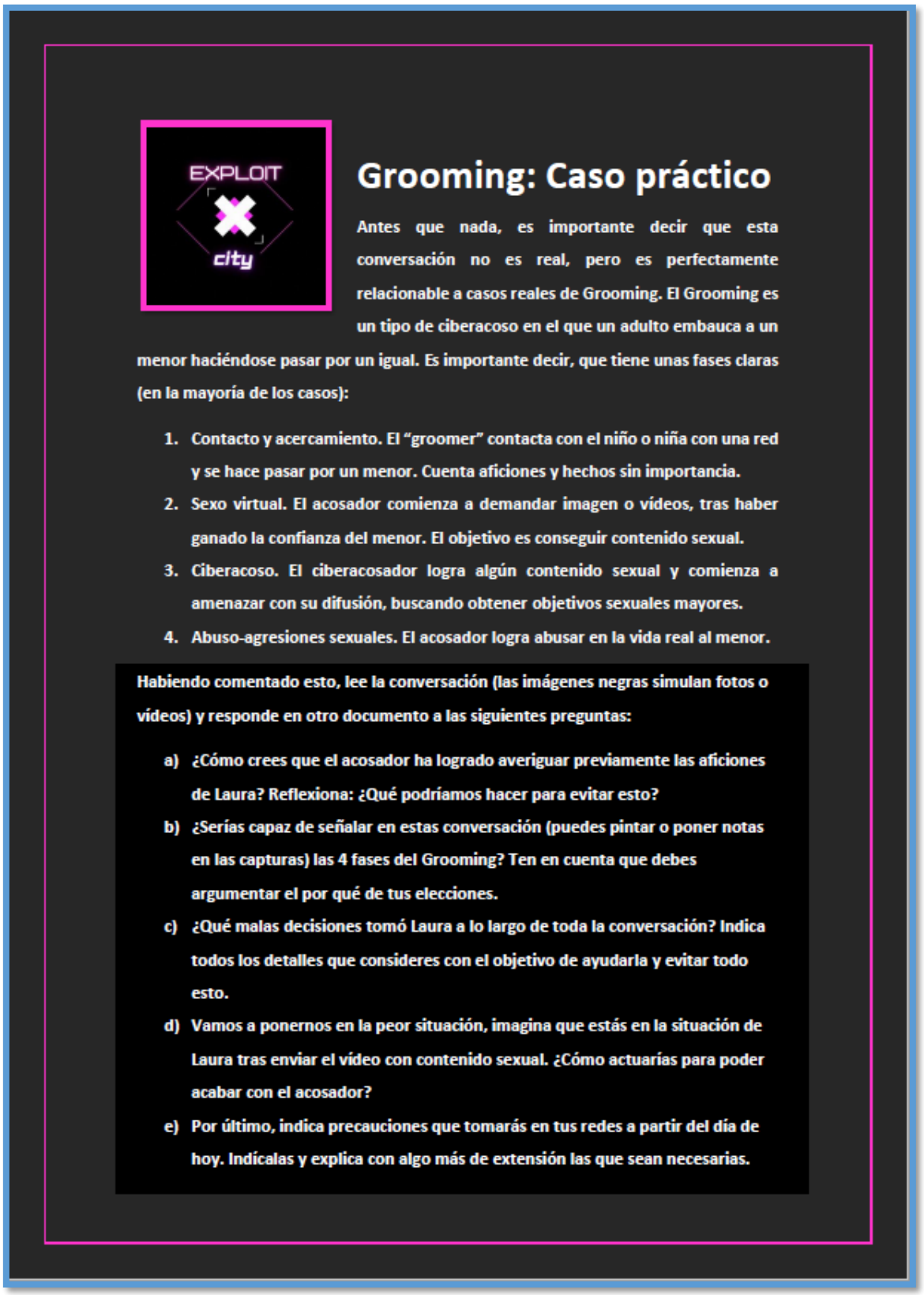
Juan Díaz y Raúl Colega, 1979, Efecto relámpago en la cara sur de la Pirámide de Keops, El poder piramidal. https://elpoderpiramidal.pdf

Por tanto, siempre tendréis que seguir esta estructura en la bibliografía:

"Nombre del autor/a o de los autores, Año, Nombre del documento o recurso, Nombre de la fuente (libro, revista, blog, web...). Enlace web".

Anexo I. Capturas de recursos de la actividad 4

Recurso 14: Fichas de cuestiones con conversaciones de WhatsApp simuladas



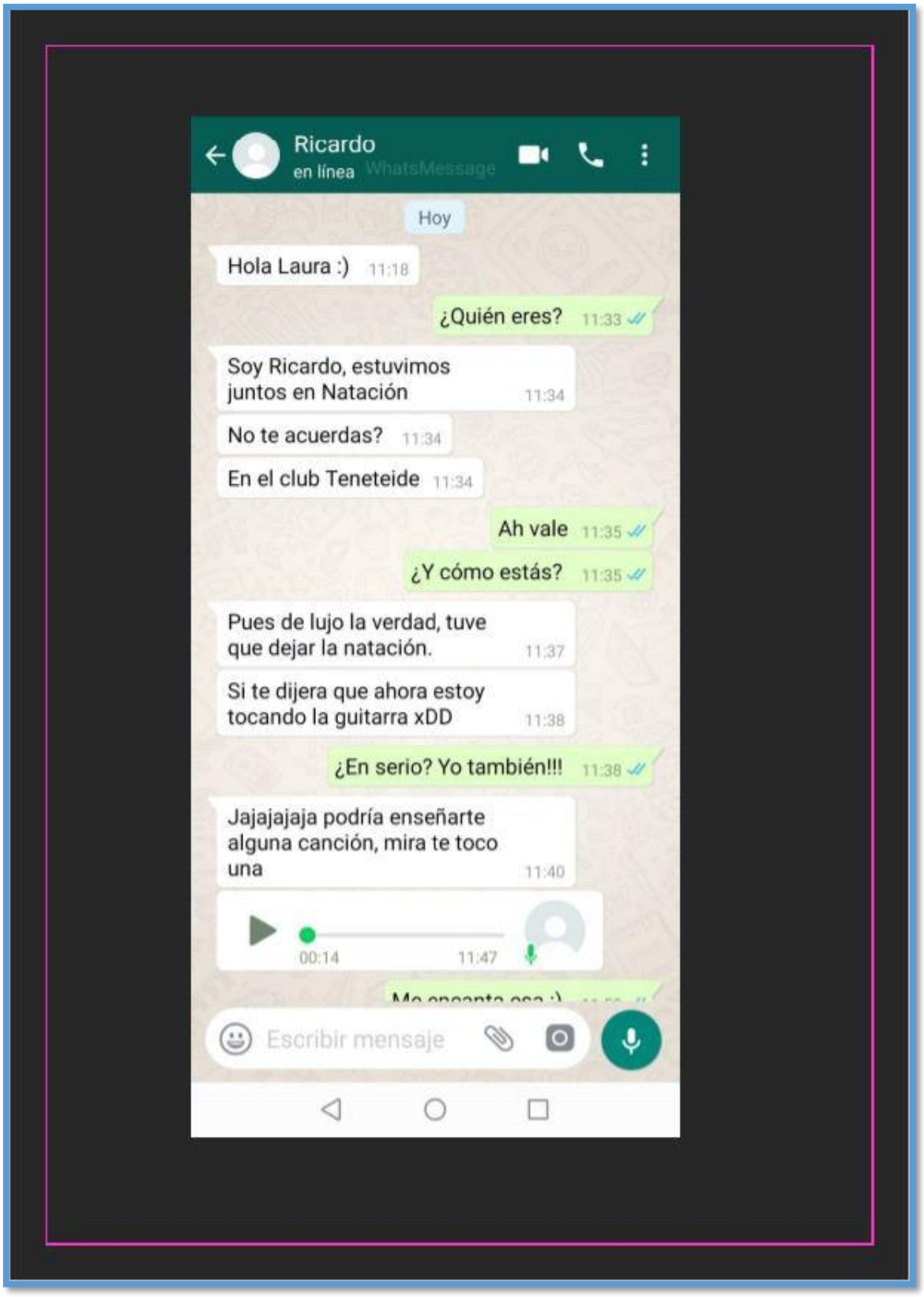
Grooming: Caso práctico

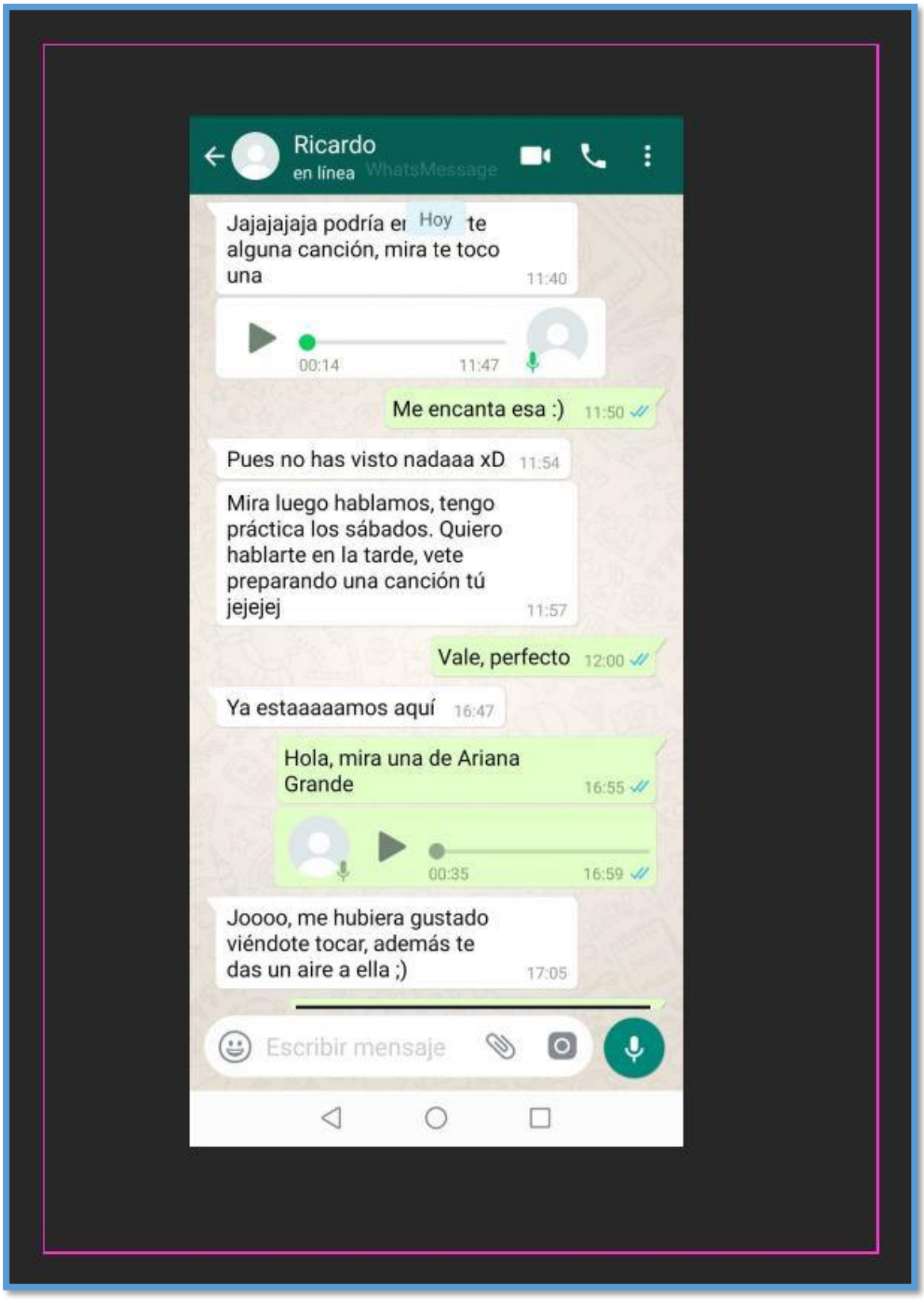
Antes que nada, es importante decir que esta conversación no es real, pero es perfectamente relacionable a casos reales de Grooming. El Grooming es un tipo de ciberacoso en el que un adulto embauca a un menor haciéndose pasar por un igual. Es importante decir, que tiene unas fases claras (en la mayoría de los casos):

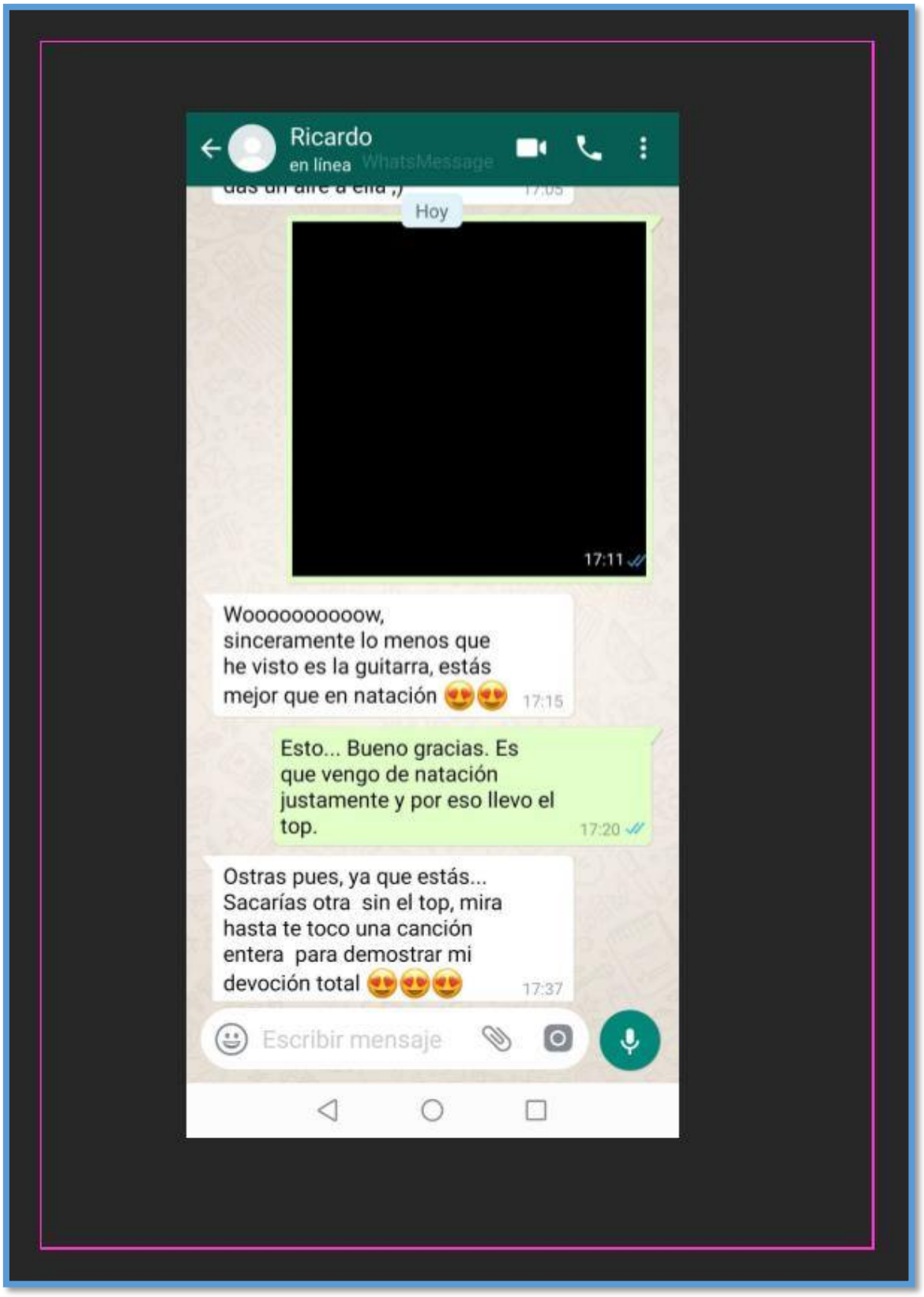
1. Contacto y acercamiento. El "groomer" contacta con el niño o niña con una red y se hace pasar por un menor. Cuenta aficiones y hechos sin importancia.
2. Sexo virtual. El acosador comienza a demandar imagen o vídeos, tras haber ganado la confianza del menor. El objetivo es conseguir contenido sexual.
3. Ciberacoso. El ciberacosador logra algún contenido sexual y comienza a amenazar con su difusión, buscando obtener objetivos sexuales mayores.
4. Abuso-agresiones sexuales. El acosador logra abusar en la vida real al menor.

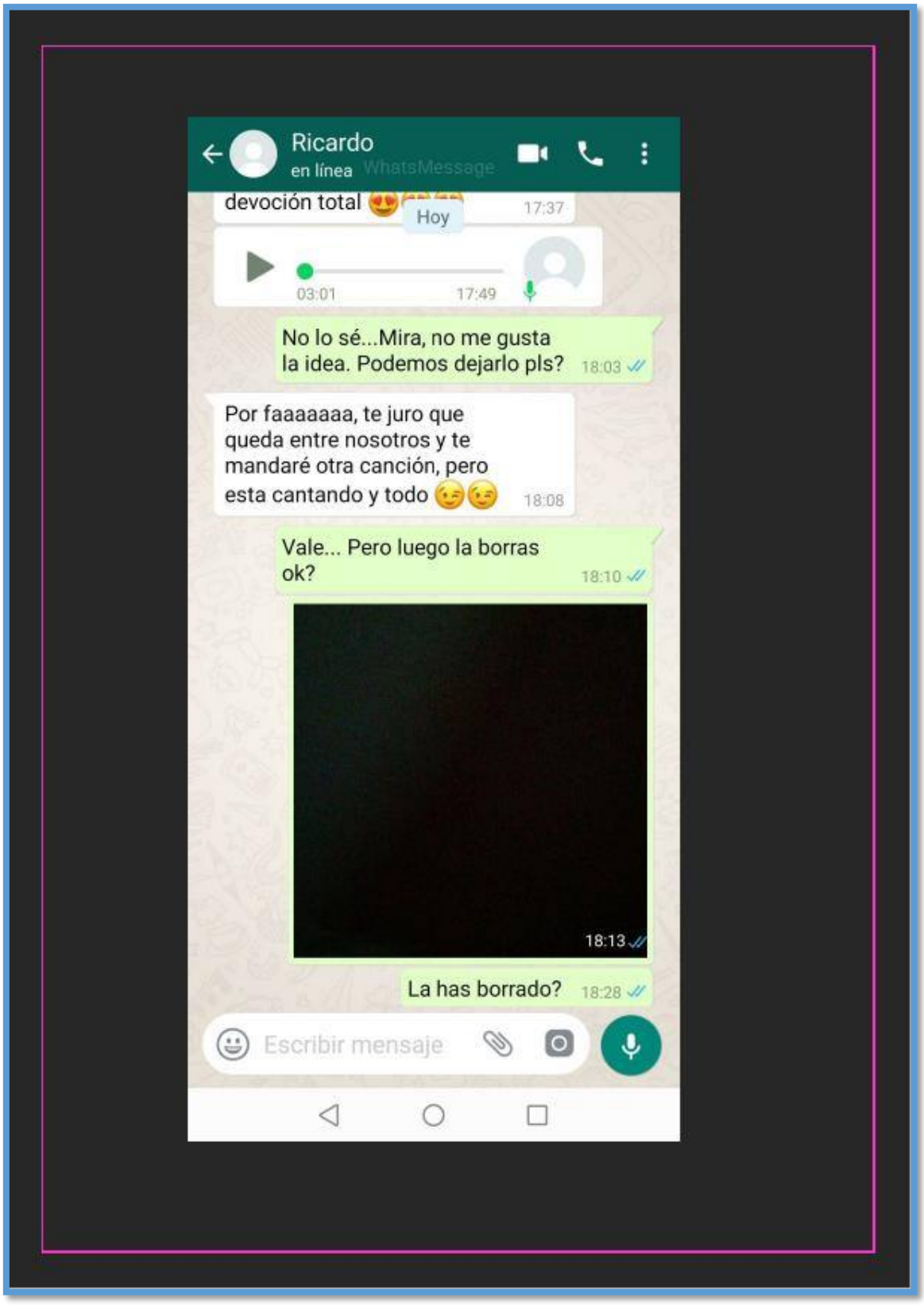
Habiendo comentado esto, lee la conversación (las imágenes negras simulan fotos o vídeos) y responde en otro documento a las siguientes preguntas:

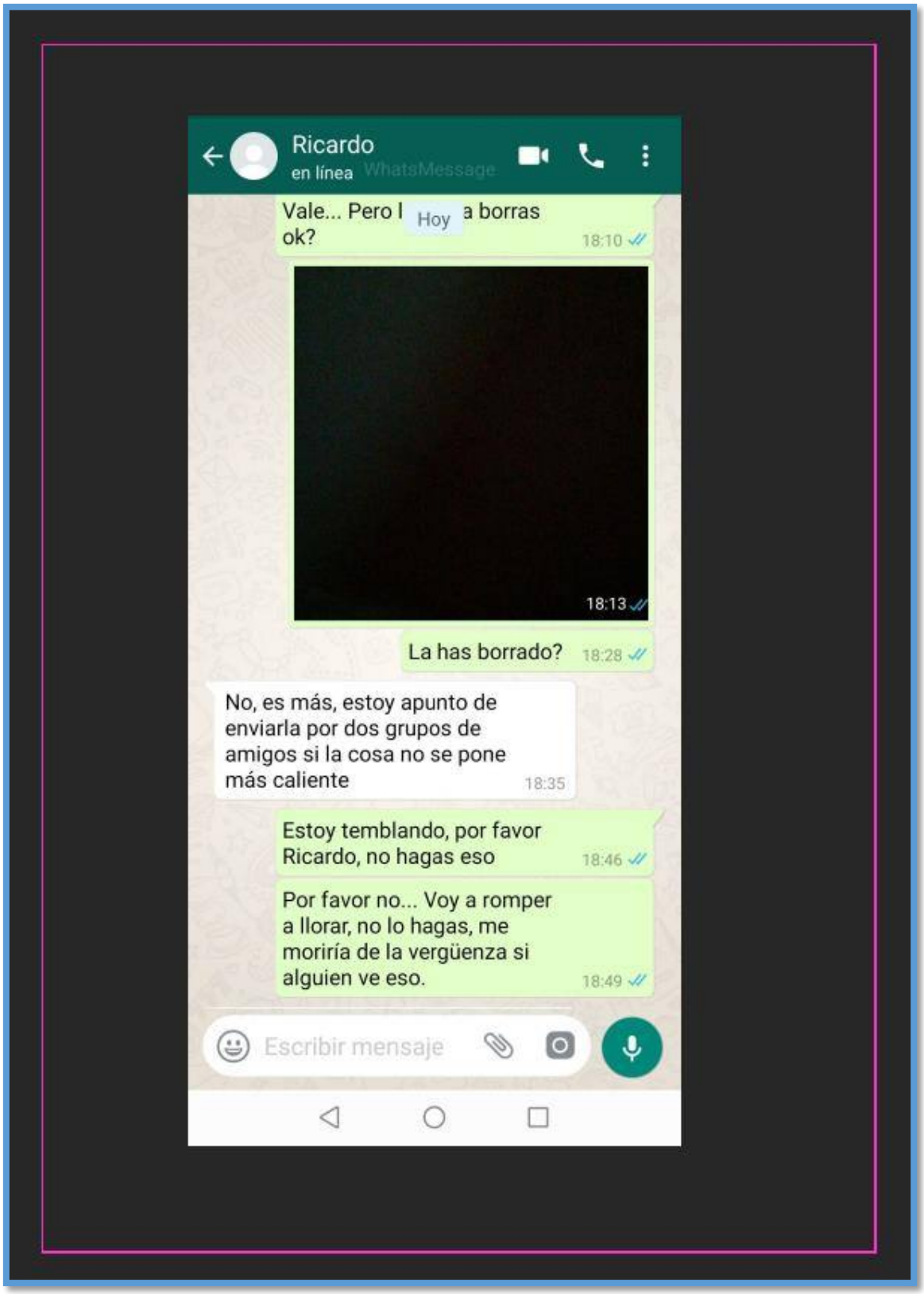
a) ¿Cómo crees que el acosador ha logrado averiguar previamente las aficiones de Laura? Reflexiona: ¿Qué podríamos hacer para evitar esto?
b) ¿Serías capaz de señalar en estas conversación (puedes pintar o poner notas en las capturas) las 4 fases del Grooming? Ten en cuenta que debes argumentar el por qué de tus elecciones.
c) ¿Qué malas decisiones tomó Laura a lo largo de toda la conversación? Indica todos los detalles que consideres con el objetivo de ayudarla y evitar todo esto.
d) Vamos a ponernos en la peor situación, imagina que estás en la situación de Laura tras enviar el vídeo con contenido sexual. ¿Cómo actuarías para poder acabar con el acosador?
e) Por último, indica precauciones que tomarás en tus redes a partir del día de hoy. Indícalas y explica con algo más de extensión las que sean necesarias.

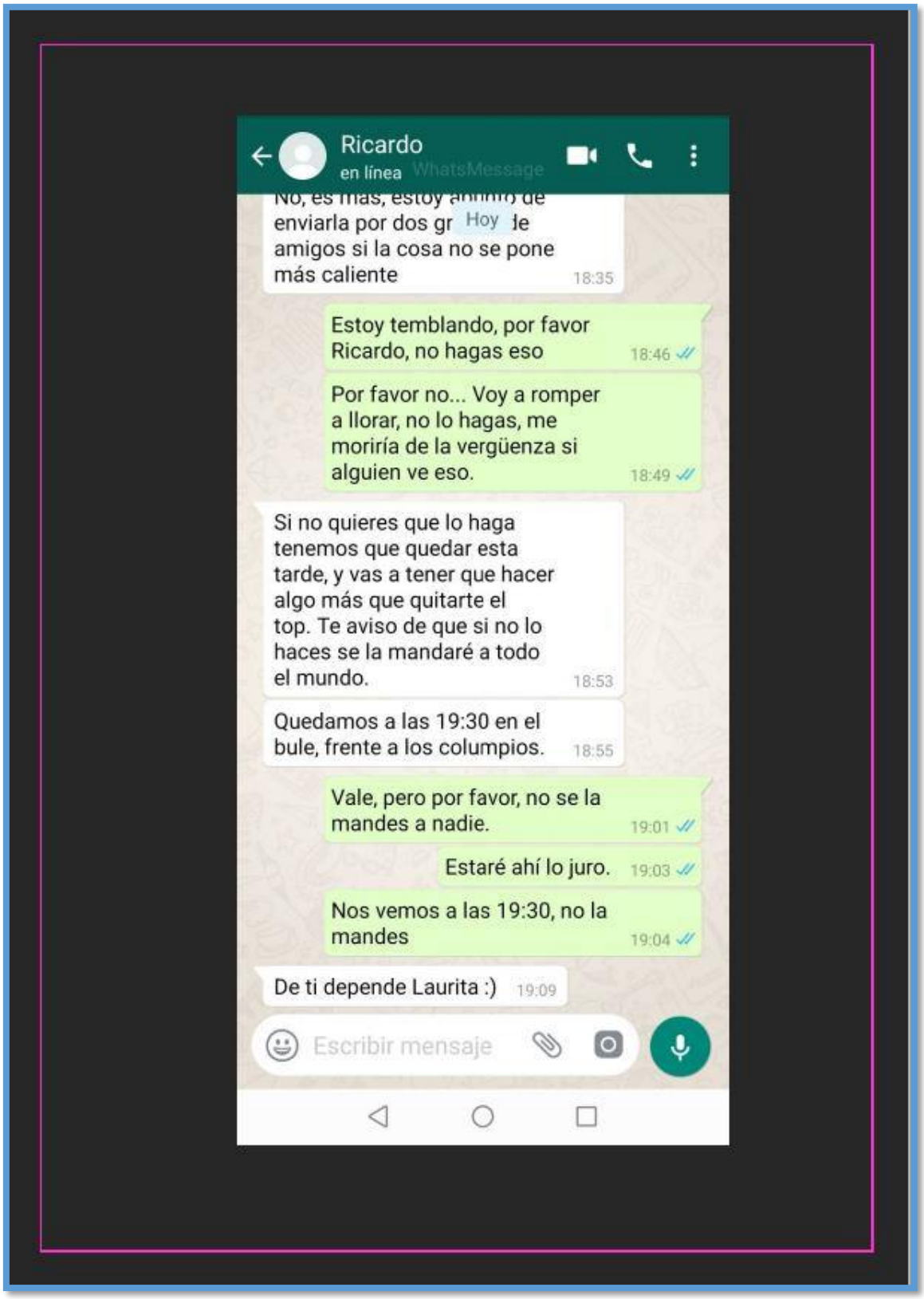

Ricardo
en línea
Hoy
Hola Laura :) 11:18
¿Quién eres? 11:33
Soy Ricardo, estuvimos juntos en Natación 11:34
No te acuerdas? 11:34
En el club Teneteide 11:34
Ah vale 11:35
¿Y cómo estás? 11:35
Pues de lujo la verdad, tuve que dejar la natación. 11:37
Si te dijera que ahora estoy tocando la guitarra xDD 11:38
¿En serio? Yo también!!! 11:38
Jajajajaja podría enseñarte alguna canción, mira te toco una 11:40
00:14 11:47
Escribir mensaje


Ricardo
en línea
WhatsMessage
Hoy
Jajajajaja podría er te alguna canción, mira te toco una
11:40
00:14
11:47
Me encanta esa :)
11:50
Pues no has visto nadaaa xD
11:54
Mira luego hablamos, tengo práctica los sábados. Quiero hablarte en la tarde, vete preparando una canción tú jejejej
11:57
Vale, perfecto
12:00
Ya estaaaaamos aquí
16:47
Hola, mira una de Ariana Grande
16:55
00:35
16:59
Joooo, me hubiera gustado viéndote tocar, además te das un aire a ella ;)
17:05
Escribir mensaje


Ricardo
en línea
Hoy
17:11
Wooooooooow, sinceramente lo menos que he visto es la guitarra, estás mejor que en natación
17:15
Esto... Bueno gracias. Es que vengo de natación justamente y por eso llevo el top.
17:20
Ostras pues, ya que estás... Sacarías otra sin el top, mira hasta te toco una canción entera para demostrar mi devoción total
17:37
Escribir mensaje

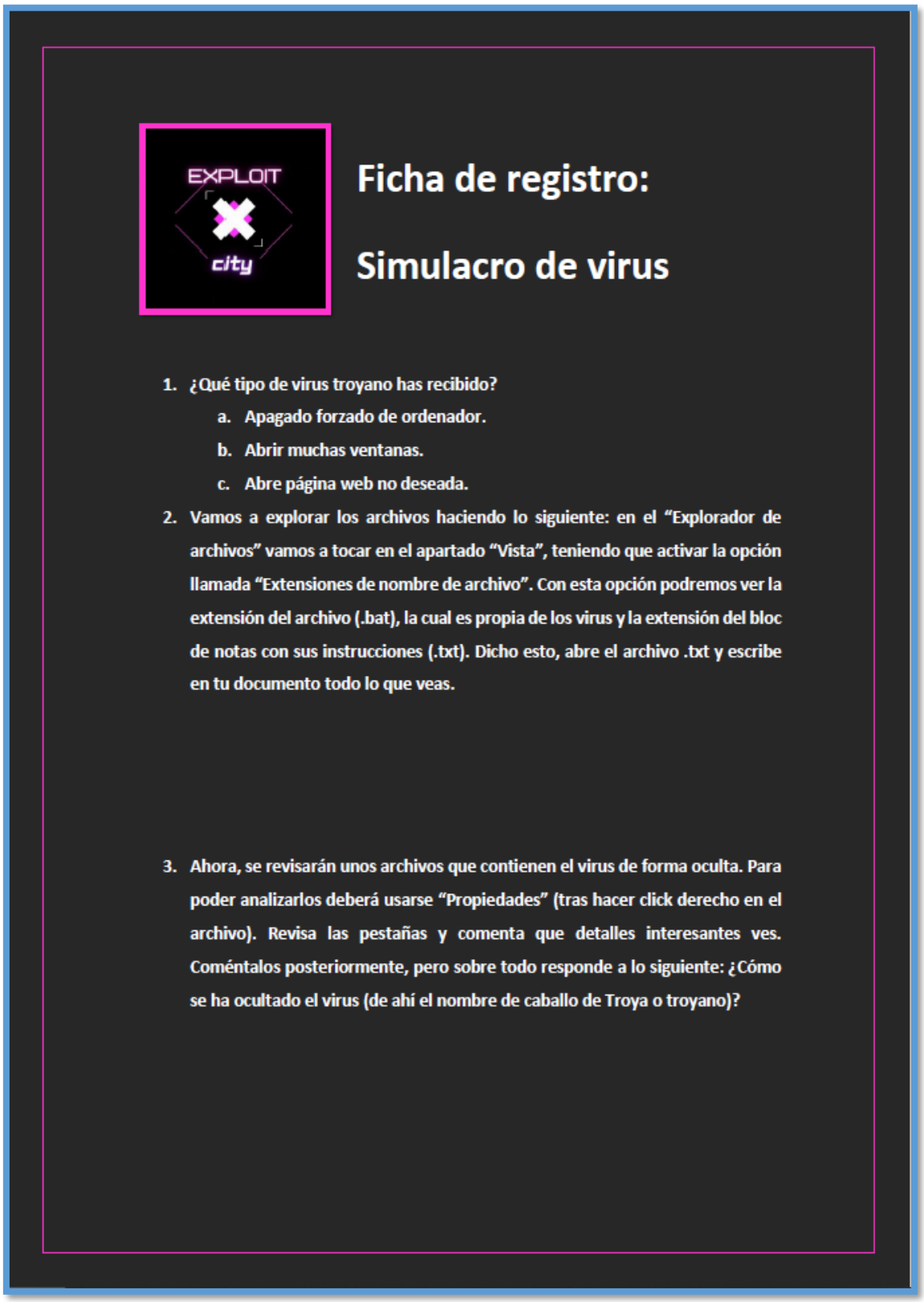

Ricardo
en línea
WhatsMessage
devoción total
17:37
Hoy
03:01
17:49
No lo sé...Mira, no me gusta la idea. Podemos dejarlo pls?
18:03
Por faaaaaaa, te juro que queda entre nosotros y te mandaré otra canción, pero esta cantando y todo
18:08
Vale... Pero luego la borras ok?
18:10
18:13
La has borrado?
18:28
Escribir mensaje


Ricardo
en línea
Vale... Pero l
Hoy
a borras
ok?
18:10
18:13
La has borrado?
18:28
No, es más, estoy apunto de enviarla por dos grupos de amigos si la cosa no se pone más caliente
18:35
Estoy temblando, por favor Ricardo, no hagas eso
18:46
Por favor no... Voy a romper a llorar, no lo hagas, me moriría de la vergüenza si alguien ve eso.
18:49
Escribir mensaje


Ricardo
en línea
WhatsMessage
enviarla por dos gr Hoy le
amigos si la cosa no se pone
más caliente 18:35
Estoy temblando, por favor
Ricardo, no hagas eso 18:46
Por favor no... Voy a romper
a llorar, no lo hagas, me
moriría de la vergüenza si
alguien ve eso. 18:49
Si no quieres que lo haga
tenemos que quedar esta
tarde, y vas a tener que hacer
algo más que quitarte el
top. Te aviso de que si no lo
haces se la mandaré a todo
el mundo. 18:53
Quedamos a las 19:30 en el
bule, frente a los columpios. 18:55
Vale, pero por favor, no se la
mandes a nadie. 19:01
Estaré ahí lo juro. 19:03
Nos vemos a las 19:30, no la
mandes 19:04
De ti depende Laurita :) 19:09
Escribir mensaje

Anexo J. Capturas de recursos de la Actividad 8

Recurso 22: Ficha de trabajo



Ficha de registro:

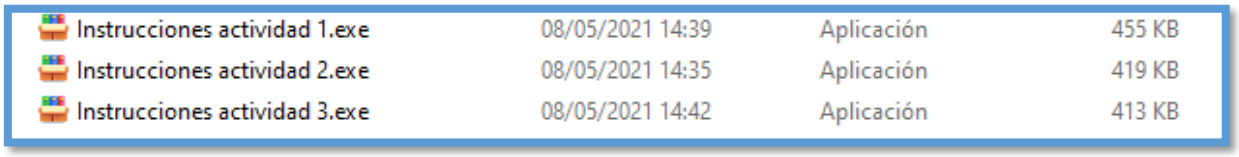
Simulacro de virus

1. ¿Qué tipo de virus troyano has recibido?
   a. Apagado forzado de ordenador.
   b. Abrir muchas ventanas.
   c. Abre página web no deseada.
2. Vamos a explorar los archivos haciendo lo siguiente: en el "Explorador de archivos" vamos a tocar en el apartado "Vista", teniendo que activar la opción llamada "Extensiones de nombre de archivo". Con esta opción podremos ver la extensión del archivo (.bat), la cual es propia de los virus y la extensión del bloc de notas con sus instrucciones (.txt). Dicho esto, abre el archivo .txt y escribe en tu documento todo lo que veas.
3. Ahora, se revisarán unos archivos que contienen el virus de forma oculta. Para poder analizarlos deberá usarse "Propiedades" (tras hacer click derecho en el archivo). Revisa las pestañas y comenta que detalles interesantes ves. Coméntalos posteriormente, pero sobre todo responde a lo siguiente: ¿Cómo se ha ocultado el virus (de ahí el nombre de caballo de Troya o troyano)?

4. Imagina otras funciones de ataque posibles para el virus troyano (ten en cuenta que este es inofensivo). ¿Cuál crees que es su nivel de peligrosidad?

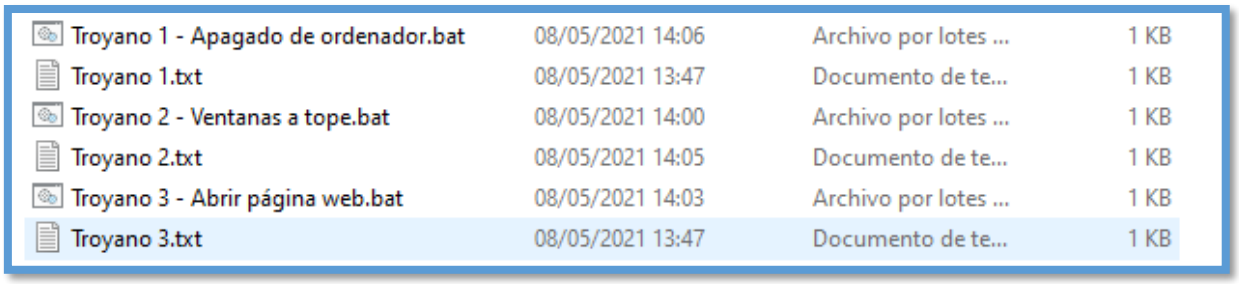
5. Por último, indica posibles medidas de protección y acción para detectar y evitar los virus. También puedes incluir las que has usado en los primeros apartados.

Recurso 23: Virus troyanos



Instrucciones actividad 1.exe	08/05/2021 14:39	Aplicación	455 KB
Instrucciones actividad 2.exe	08/05/2021 14:35	Aplicación	419 KB
Instrucciones actividad 3.exe	08/05/2021 14:42	Aplicación	413 KB

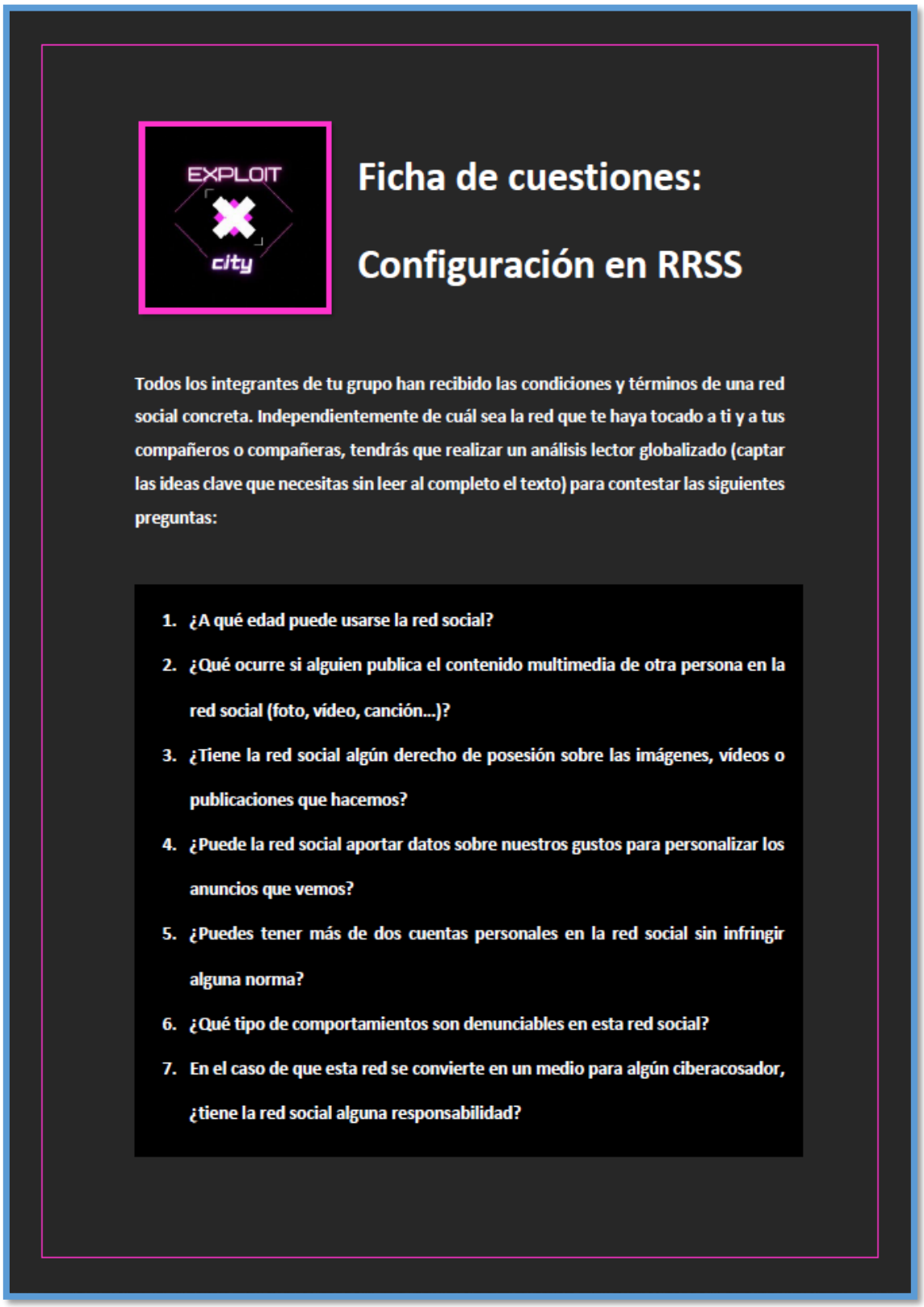
Recurso 24: Ficheros de los virus



Troyano 1 - Apagado de ordenador.bat	08/05/2021 14:06	Archivo por lotes ...	1 KB
Troyano 1.txt	08/05/2021 13:47	Documento de te...	1 KB
Troyano 2 - Ventanas a tope.bat	08/05/2021 14:00	Archivo por lotes ...	1 KB
Troyano 2.txt	08/05/2021 14:05	Documento de te...	1 KB
Troyano 3 - Abrir página web.bat	08/05/2021 14:03	Archivo por lotes ...	1 KB
Troyano 3.txt	08/05/2021 13:47	Documento de te...	1 KB

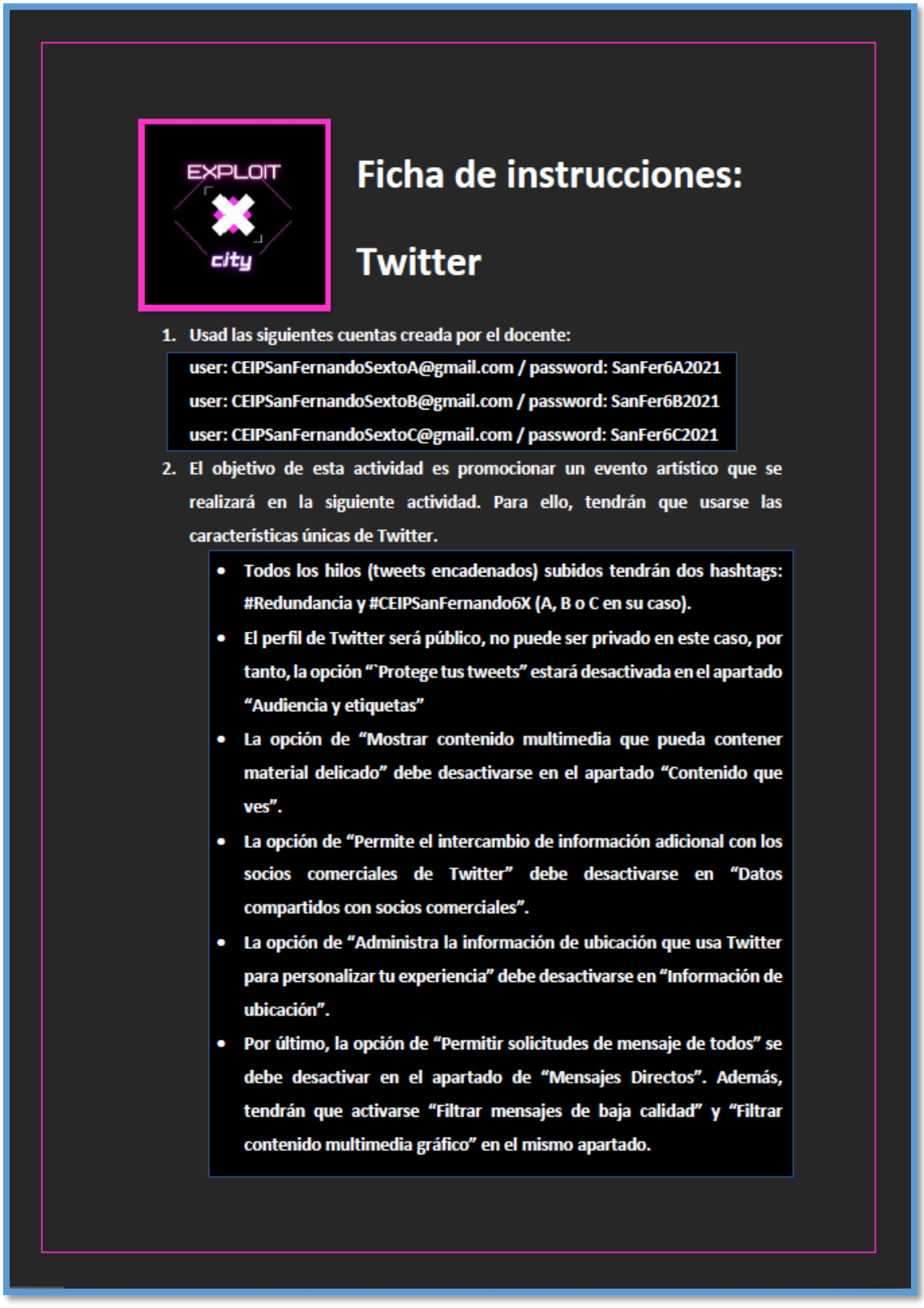
Anexo K. Capturas de recursos de la actividad 10

Recurso 31: Ficha de cuestiones



Anexo L. Capturas de recursos de la actividad 11

Recurso 33: Instrucciones del grupo Twitter



3. Las promociones se realizarán aplicando la siguiente estrategia publicitaria:

Hilos promocionales / campañas publicitarias en hilo. Tenéis que hacer 4 mini-historias para promocionar la actividad "Redundancia", la cual será comentada en clase. Las historias se redactarán en un documento por separado, y la dificultad es que tienen que finalizar con una frase final muy peculiar (leer siguiente estrategia).

Eslogan. Son frases breves y originales, las cuales cuentan con un efecto atractivo para el público. Estas frases deben finalizar las 4 mini-historias, por tanto, deben existir 4 eslóganes finalizando cada hilo de Twitter.

Recurso 34: Instrucciones del grupo TikTok

Ficha de instrucciones:

TikTok

1. Usad las siguientes cuentas creada por el docente:

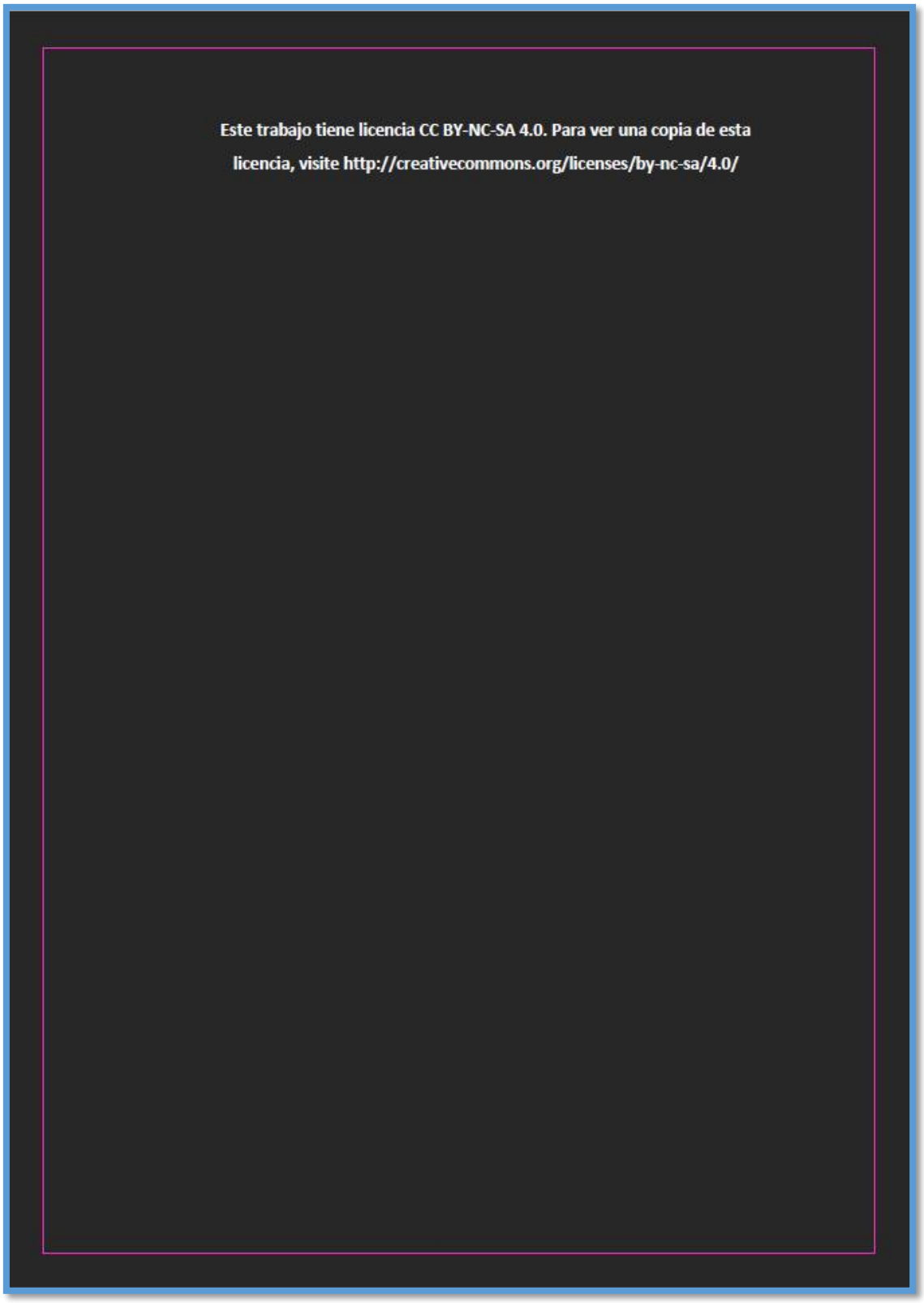
user: CEIPSanFernandoSextoA@gmail.com / password: SanFer6A2021
user: CEIPSanFernandoSextoB@gmail.com / password: SanFer6B2021
user: CEIPSanFernandoSextoC@gmail.com / password: SanFer6C2021

2. El objetivo de esta actividad es promocionar un evento artístico que se realizará en la siguiente actividad. Para ello, tendrán que usarse las características únicas de TikTok.

- Al subir vídeos tendrán que emplearse los siguientes permisos:
  - Pueden ver vídeos todas las personas (público).
  - Se permite a usuarios externos reaccionar ("Reaccionar/ Hacer dúos") y comentar ("Comentario"), pero no extraer clips de los vídeos subidos ("Pegar").
- El perfil debe estar en privado, usando la "Configuración".
- Todos los vídeos subidos tendrán dos hashtags: #Redundancia y #CEIPSanFernando6X (A, B o C en su caso).

3. Las promociones se realizarán aplicando la siguiente estrategia publicitaria:

Anuncios. Tendréis que realizar 4 anuncios de entre 40 - 60 segundos para promocionar el evento que comentaremos en clase. Todos y todas las integrantes deben salir en el vídeo. Es importante redactar un guion para que el anuncio esté correctamente organizado y pautado. Estos anuncios pueden ser vistos por cualquiera, no obstante, se mandarán enlaces a las familias y otros agentes del centro para que puedan verlo con toda seguridad (asegurando reacciones y comentarios).


Este trabajo tiene licencia CC BY-NC-SA 4.0. Para ver una copia de esta
licencia, visite http://creativecommons.org/licenses/by-nc-sa/4.0/

Recurso 35: Instrucciones del grupo Pinterest

Ficha de instrucciones:

Pinterest

1. Usad las siguientes cuentas creada por el docente:

user: CEIPSanFernandoSextoA@gmail.com / password: SanFer6A2021
user: CEIPSanFernandoSextoB@gmail.com / password: SanFer6B2021
user: CEIPSanFernandoSextoC@gmail.com / password: SanFer6C2021

2. El objetivo de esta actividad es promocionar un evento artístico que se realizará en la siguiente actividad. Para ello, tendrán que usarse las características únicas de Pinterest.
   - Accediendo al apartado de "Privacidad y datos", debemos hacer lo siguiente: en "@Mentions" debemos activar "Solo a personas a las que sigas" y en "Personalización" debemos desactivar todas las opciones.

3. Las promociones se realizarán aplicando la siguiente estrategia publicitaria:

Tableros publicitarios. Los pines que se colocarán en el tablero serán anuncios publicitarios creativos escritos a mano. Primero tendrán que redactarse un total de 3 por integrante (no deben tener más de 7 líneas cada uno). Posteriormente se les sacará en una foto, y todos se meterán en un tablero llamado "Redundancia", el cual contendrá sub-tableros con el nombre de cada integrante y sus anuncios subidos como pines. De esta manera, se sabrá a quién pertenece cada anuncio.

Recurso 36: Instrucciones del grupo Instagram

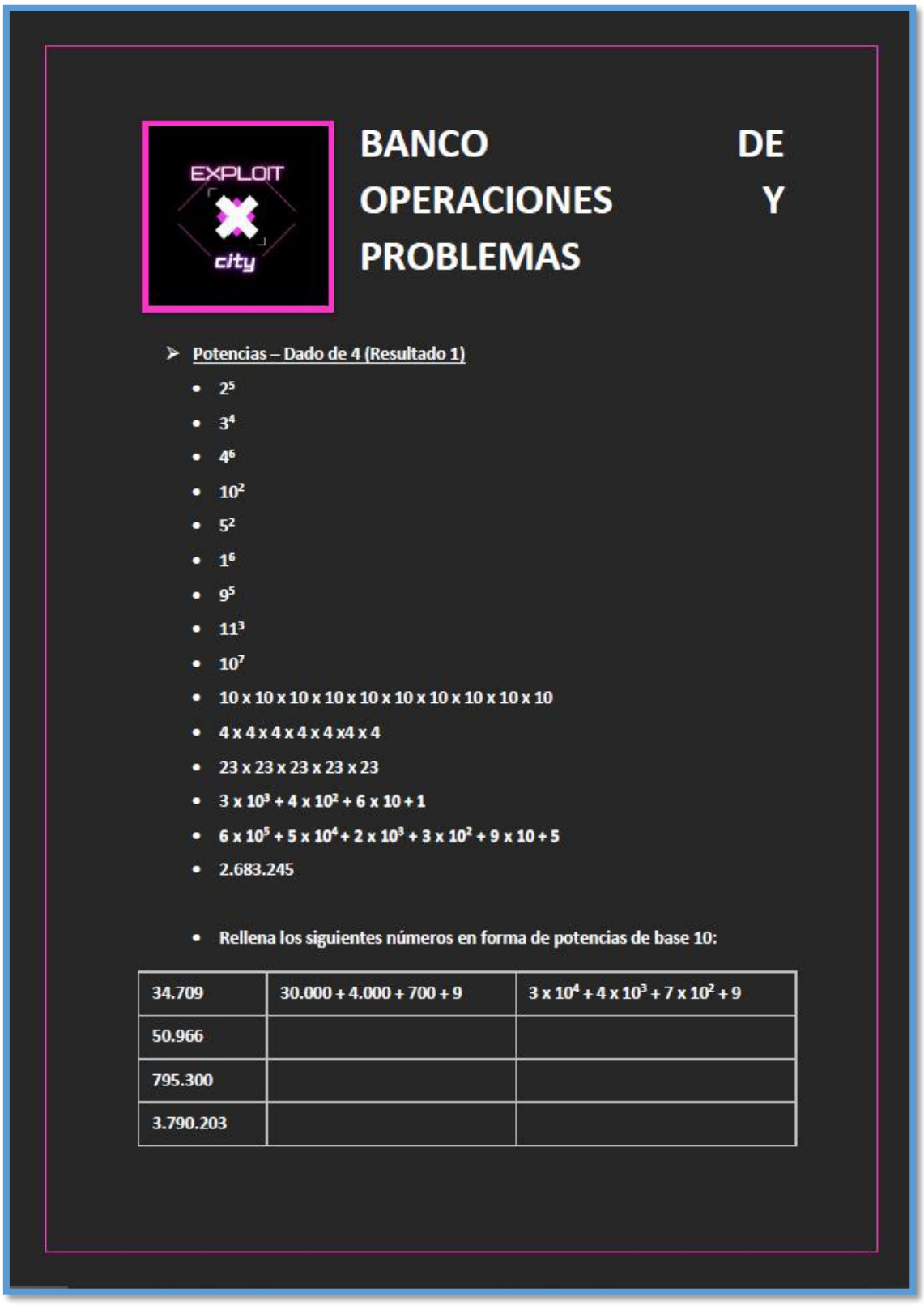
Recurso 37: Instrucciones del grupo Facebook

3. Las promociones se realizarán aplicando la siguiente estrategia publicitaria:

Grupo promocional. Se creará un grupo abierto, en el cual se harán publicaciones para anunciar el evento. Dichas publicaciones deben tener un formato de anuncio promocional, en el cual se busca un público objetivo (por ejemplo, las familias). Por tanto, el diseño del anuncio debe varias en función de las personas que reciban la promoción de "Redundancia" (el evento a promocionar). Cada integrante planeará 4 anuncios para un público distinto, con el objetivo de atraerlos a dicho grupo.

Anexo M. Capturas de recursos de la actividad 13

Recurso 33: Instrucciones del grupo Twitter



BANCO DE OPERACIONES Y PROBLEMAS

- Potencias – Dado de 4 (Resultado 1)
  - 2^5
  - 3^4
  - 4^6
  - 10^2
  - 5^2
  - 1^6
  - 9^5
  - 11^3
  - 10^7
  - 10 x 10 x 10 x 10 x 10 x 10 x 10 x 10 x 10 x 10
  - 4 x 4 x 4 x 4 x 4 x4 x 4
  - 23 x 23 x 23 x 23 x 23
  - $3 \times 10^3 + 4 \times 10^2 + 6 \times 10 + 1$
  - $6 \times 10^5 + 5 \times 10^4 + 2 \times 10^3 + 3 \times 10^2 + 9 \times 10 + 5$
  - 2.683.245

- Rellena los siguientes números en forma de potencias de base 10:

34.709	30.000 + 4.000 + 700 + 9	$3 \times 10^4 + 4 \times 10^3 + 7 \times 10^2 + 9$
50.966		
795.300		
3.790.203		

- **Lucía tuvo 4 hijas. Cada una de ellas tuvo 4 hijas, y cada una de estas tuvo otras 4 hijas. ¿Cuántas nietas tuvo Lucía?**

- **Un solar de gran tamaño contiene 7 edificios. Cada uno de estos edificios tiene 7 pisos y todos estos estos tienen 7 ventanas. ¿Cuál es el total de ventanas de los edificios?**

- **Expresa las siguientes cifras en potencias de base 10:**

100 =	1.000 =	1.000.000 =
100.000 =	1.000.000.000 =	10.000 =

- **Completa la siguiente tabla:**

Producto	Base	Exponente	Potencia	Se lee
5 x 5 x 5				
	3	7		
				1 elevado a 6

➢ **Jerarquía de operaciones – Dado de 4 (Resultado 2)**

- **200 / 2 / 25 + 3**
- **5 – 3 – 2 x 2**
- **3 + 5 x (–7 – 3)**
- **4 + 2 · [3 + 2 – (4 – 1)]**
- **5 x (12 / 3) + 3 x (19 – 16)**
- **23 – 2 x (4 + 28) / 4**
- **3 x (2 + 3 – 4) – 40 / 10**
- **(7 x 2) + (4 x 5) – 3**
- **(42 – 26) – 10 x (2 + 12) / 2**

- (21 + 13) x 4 – 72 / 4
- 21 x (7 + 28) / 4 – (300 / 25)
- 325 x (20 – 12) + 144/12
- [(92 + 3) /5] x (21 – 7)
- 27 x [(5 + 164) / 13] + (450 / 45)
- 1 + 2 x 4 (- 49 / 7 - 14) x 112
- 404 / (578 – 477) + 32 x (-5) – 7
- 440 – [30 + 6 - (9 x 4)]
- 332 – 44 x 3 – (440 /4)
- 712 – [(34-28) x 3 + 4 x (110 /2 + 5)]
- [(27 x 22) / 6] – 7 x (12 +3)

➢ Porcentajes y Regla de 3 (Resultado 3)

- 28% de 400
- 60% de 120
- 30% de 27
- 42% de 525
- 20% de 360
- 95% de 1412
- 31% de 321
- X % de 125 = 25
- X % de 100 = 35
- X % de 200 = 48

- En una empresa, cuatro ordenadores producen 1500 informes de diagnóstico en 2 horas. ¿Cuántos informes se producirán en 9 horas? Uno de los ordenadores se ha averiado, ¿cuántas horas se necesitarán para alcanzar la misma cantidad de informes que en 9 horas con dos ordenadores?

- Un empleado que cobra 1400 euros mensuales ha conseguido un aumento de salario del 7%. ¿Cuánto dinero va a cobrar a partir de ahora?

- Una profesora ha corregido 28 exámenes en dos días. ¿Cuántos exámenes podrá corregir en un total de 27 días?

- Un coche que va a 40 km por hora (velocidad) tarda 30 minutos en hacer un recorrido. ¿Cuánto tiempo tardará en hacer el mismo recorrido si va a 120 km por hora?

- Dos empleados limpian una piscina en 30 minutos, ¿si aumentamos los empleados a 6 cuánto tiempo tardarían?

➢ <u>Fracciones – Dado de 4 (Resultado 4)</u>

- 6/7 – 3/8
- 4/4 – 1/6
- 5/6 – 1/8
- 2/10 – 1/12
- 11/15 – 3/8
- 8/10 – 1/4
- 1/5 + 4/3
- 8/6 + 2/7
- 1/4 + 4/9
- 1/2 + 3/2
- 34/3 + 7/4
- 65/100 + 767/1000
- 4/3 – 23/24
- 300/1000 – 7373/10000
- 92/3 – 3/4

- Para celebrar el cumpleaños de Mario, algunas de sus amigas y amigos decidieron reservar en un restaurante. Teniendo en cuenta que cada uno invirtió de forma distinta al comprar los regalos, a la hora de pagar la reserva lo dividieron de forma diferente para que fuera más equitativo. Anabel tuvo que pagar 1/15 del total; Juan, 1/6; Alicia, 1/5; Miguel 1/10; Alfredo 2/15. Como Rafael no compró regalo, pagó el resto. ¿Qué fracción del total le tocó pagar a Rafael?

- La cocina del Hotel Mencey debe cocinar un plato para un crítico de cocina de Michelín. El tiempo es oro, y los cocineros han de preparar un Sancocho Canario en 30 minutos. Disponen de 1/4 del tiempo para la elaboración de la salsa. Por otro lado, 2/8 de ese tiempo deben dedicarse a la cocción de las papas de acompañamiento. ¿Cuánto es el tiempo total gastado en la elaboración de la salsa y las papas? Es importante tener en cuenta, que el pescado en 2/4 necesita de 150º centígrados de temperatura en el horno. Habiendo calculado el dato anterior, ¿cuánto tiempo le queda para hornear el pescado? En caso de tener menos tiempo, ¿cuánto tendríamos que aumentar la temperatura del horno?

- Un grupo de niños/as han montado un puesto de limonada en la calle Herradores. Sabiendo que la limonada tiene por cada litro los siguientes ingredientes: 2/10 de su contenido es de agua y 14/20 es limón exprimido, el resto son azúcares. ¿Cuántas cantidades de azúcar lleva un litro de limonada?

- En el bar de Juan, venden pollo asado por trozos. Asimismo, cada pollo se divide en 8 piezas distintas. En un intervalo de media hora se encargan por teléfono las siguientes cantidades: 1/2 pollo para Antonio Fernández, 3/4 para Juan Sánchez, 5/8 para Virginia Díaz y 6/2 para Manuel Pérez ¿Cuántos pollos se deben sacar de la cámara? En el caso de que sobren algunas piezas de un pollo ¿Cuál sería el porcentaje sobrante?

- **Los ingresos del restaurante Da Angeló se dividen en lo siguiente: 2/5 se obtienen por la comida servida en el restaurante, 1/4 se debe a la comida a domicilio y el resto se debe a la propina dejada por los/as clientes/as. ¿Qué fracción de los ingresos totales se deben a la propina? Exprésala de forma irreducible.**

NOTA IMPORTANTE: Una vez el discente informe del resultado del dado de 4, el docente lanzará un dado de 20 para tomar el ejercicio o problema a realizar. Dicha selección no volverá a ser elegible por el azar. Por tanto, cuando empiecen a salir varias repeticiones en los lanzamientos, el docente podrá tomar los que no hayan salido previamente. Así hasta finalizar el proyecto, no el banco (el banco está preparado con muchas operaciones y problemas para realizar, pero no es obligatorio hacerlo todo).

Anexo N. Justificación legal de uso de RRSS (Acts. 11 y 12)

Estimadas familias:

Como tutor se contacta con ustedes porque, en las próximas semanas, van a trabajarse una serie de contenidos relacionados con la ciberseguridad en la red. Dicha temática se aborda con el objetivo de garantizar la protección de sus hijos e hijas mientras usan dispositivos tecnológicos, ya sea en el centro, en casa o en cualquier otro espacio.

Es importante indicar que van a utilizarse cinco redes sociales (Twitter, Facebook, TikTok, Instagram y Facebook) a través de una cuenta creada por el docente. En ningún caso los menores crearán una cuenta personal en las actividades. No obstante, es necesario solicitar una serie de permisos para hacer un uso educativo. Deben saber que pueden aceptar o denegar (marcar casilla final) los que ustedes consideren:

D./Dña. _____

con DNI _____, padre, madre o tutor/a legal del menor _____, consiente o autoriza:

☐ El uso de redes sociales con fines educativos y didácticos. Posteriormente, las cuentas quedarán inhabilitadas, siendo imposible su uso.

☐ El uso de material audiovisual en el que puedan aparecer sus hijos e hijas, teniendo todo fin de divulgación y comunicación un carácter educativo pleno. Todos estos materiales serán enviados a las familias para su visionado y serán eliminados de la red al finalizar el proyecto.

☐ No autorizo ninguno de los dos usos anteriores.

Firmado: ☐

CEIP San Fernando a día ___ de _____ del año _____

Anexo O. Recursos físicos de “Exploit City”: Dados de rol

Cada alumno y alumna dispondrá de estos dados:

- Dado de 4
- Dado de 6
- Dado de 8
- Dado de 10
- Dado de 12
- Dado de 20

Anexo P. Manual de la gamificación “Exploit City”

Índice

1. Diseño de personaje

"Exploit City" cuenta con unas características únicas en cuento a su sistema de creación de personaje. Es momento de abordar cada uno de ellos por separado.

1.1. Clases de personaje

Las clases de jugador van a quedar íntimamente relacionadas a los roles de los grupos cooperativos. De esta forma se eliminan las posibles discusiones por la elección de las clases, las cuales tienen una serie de habilidades y objetos únicos. No obstante, hay que decir que todas ellas tienen una enorme utilidad dentro de la historia gamificada. Es momento de desarrollarlas:

- ***"Leader" (Coordinador/a).*** Su misión es velar por correcto funcionamiento de los distintos roles, dejando claro en todo momento el objetivo de cada misión. Sus habilidades tienen que ver con la potenciación y la inspiración de sus compañeros/as. Además, también puede rebajar el poder y la defensa enemiga.
- ***"Fixer" (Crítico/a).*** Su objetivo es velar por la correcta realización de tareas y actividades. Cualquier error que no sea corregido por el resto de los integrantes será depurado por un jugador o jugadora de esta clase. Sus habilidades están relacionadas con la evaluación y planificación de riesgos.
- ***"Corpo" (Secretario/a).*** Encargado del registro de las distintas actividades. A pesar de estar encargado de la redacción, debe recibir colaboración del resto de sus compañeros y compañeras de equipo. Sus habilidades tienen que ver con la potencia física y con la protección defensiva.
- ***"Link" (Portavoz).*** Su misión es transmitir las opiniones, resultados y avances de todo el grupo. Su clase conlleva un mayor uso de la palabra que en cualquiera de las otras, aunque existan momentos en los que tengan que participar en igualdad de tiempos. Sus habilidades se basan en la persuasión e intimidación.
- ***"Netrunner" (Controlador/a).*** Se encarga de organizar y planificar los materiales y pasos a seguir en cada trabajo a realizar, subdividiendo correctamente los recursos necesarios para cada integrante. Además, controla los tiempos de las entregas. Sus habilidades se relacionan al hackeo y el control de dispositivos.

1.2. Inventario de inicio

- **Inventario de inicio de la clase "Leader"**
  - ✓ 3 pociones de 1d6
  - ✓ 1 poción de 1d8
  - ✓ Pistola eléctrica. 1d6 de daño. Existen 4 mejoras disponibles en los mapas: +1 de daño por mejora.
  - ✓ Blindaje de nivel 1. 12 de armadura. Existen 2 mejoras disponibles en los mapas: +1 de armadura por mejora.
- **Inventario de inicio de la clase "Fixer"**
  - ✓ 3 pociones de 1d6
  - ✓ 1 poción de 1d8
  - ✓ Desintegrador de materia. 1d6 de daño. Existen 4 mejoras disponibles en los mapas: +1 de daño por mejora.
  - ✓ Blindaje de nivel 1. 12 de armadura. Existen 2 mejoras disponibles en los mapas: +1 de armadura por mejora.
- **Inventario de inicio de la clase "Corpo"**
  - ✓ 3 pociones de 1d6
  - ✓ 1 poción de 1d8
  - ✓ Puños biónicos. 1d6 de daño. Existen 4 mejoras disponibles en los mapas: +1 de daño por mejora.
  - ✓ Blindaje de nivel 1. 12 de armadura. Existen 2 mejoras disponibles en los mapas: +1 de armadura por mejora.
- **Inventario de inicio de la clase "Link"**
  - ✓ 3 pociones de 1d6
  - ✓ 1 poción de 1d8
  - ✓ Controlador de CPU (mente de un robot o dispositivo). 1d6 de daño. Existen 4 mejoras disponibles en los mapas: +1 de daño por mejora.
  - ✓ Blindaje de nivel 1. 12 de armadura. Existen 2 mejoras disponibles en los mapas: +1 de armadura por mejora.

- **Inventario de inicio de la clase "Netrunner"**
  - ✓ 3 pociones de 1d6
  - ✓ 1 poción de 1d8
  - ✓ Ordenador maestro: 1d6 (4 mejoras disponibles en los mapas: +1 de daño por mejora)
  - ✓ Blindaje de nivel 1. 12 de armadura. Existen 2 mejoras disponibles en los mapas: +1 de armadura por mejora.
  - ✓ Programas para hackear:
    - "Revability": Revelar habilidad de carga.
    - "Vision": Control de cámara o dron.

1.3. Estadísticas principales

Las estadísticas son:

- ***Fuerza (FUE).*** Mide la potencia física, entrenamiento deportivo y situaciones en que se puede ejercer potencial físico.
- ***Destreza (DES).*** Mide la agilidad y los reflejos.
- ***Constitución (CON).*** Mide la resistencia en cualquier actividad.
- ***Inteligencia (INT).*** Mide el razonamiento y la memoria.
- ***Sabiduría (SAB).*** Mide la perspicacia, la intuición y la capacidad de planificación.
- ***Carisma (CAR).*** Mide la capacidad para interactuar correctamente (elocuencia y confianza) con otros seres.

Estas estadísticas tienen un valor de 5 como mínimo. Sin embargo, en función de la clase hay dos que tendrán un valor de 7.

- **Los/as "netrunners"** tendrán 7 en Destreza y Sabiduría.
- **Los/as "fixers"** tendrán 7 en Inteligencia y Sabiduría.
- **Los/as "links"** tendrán 7 en Carisma y Constitución.
- **Los/as "corpos"** tendrán 7 en Fuerza y Constitución.
- **Los/as "leaders"** tendrán 7 en Inteligencia y Carisma.

Por otro lado, hay otras estadísticas, las cuales denominaremos "vitales". Estas son:

- ***Puntos de vida (PV).*** Serán en inicio 15, y aumentarán en +2 con cada nivel. Podrán restaurarse con pociones o momentos de trabajo.
- ***Defensa (DEF).*** Tendrá el mismo valor que la armadura equipada. Este valor tendrá que ser superado por el enemigo con el dado de 20 (icosaedro) para poder golpear.
- ***Inspiración (INS).*** Al resolver una actividad de forma creativa, mediar un conflicto satisfactoriamente o ayudar a un compañero o compañera de forma eficaz, podrá obtenerse una ventaja de inspiración. Esto asegura que podrá usarse ese punto (una sola vez) para atacar antes o salvar a un miembro de perder sus últimos puntos de vida.

1.4. Habilidades

Cada grupo tendrá un máximo de 6 usos de habilidades por cada corporativa. No pueden recuperarse con ninguna poción no objeto. Dicho esto, es tiempo de comenzar con el desarrollo de las habilidades de cada clase. La relación existente con el sistema de niveles quedará explicada posteriormente.

- Habilidades de la clase "Leader":
  - ✓ **Nivel 1 – Guía de líder**. Los aliados acertarán todos los ataques sin necesidad de usar el dado de 20 durante un turno.
  - ✓ **Nivel 2 – Ataque inspirador**. El/la líder potenciará en +2 su ataque en ese mismo turno.
  - ✓ **Nivel 3 – Intimidación de jefe.** Se intimida a un enemigo o un grupo de estos, evitando sus ataques durante un turno.
  - ✓ **Nivel 4 – Destrozo mental**. La defensa de cualquier enemigo baja 3 puntos.
- Habilidades de la clase "Fixer":
  - ✓ **Nivel 1 – Plan de riesgo**. Garantiza que nadie muere en un turno, manteniendo 1 punto de vida a todos los aliados.
  - ✓ **Nivel 2 – Desorganización organizada.** Se desordenan muchos objetos para generar un estado de confusión a los enemigos.

- ✓ **Nivel 3 – Oportunista.** Atacas al punto más vulnerable de un enemigo, duplicando el daño de tu arma. Por ejemplo, si es de1d6, pasaría a ser de 1d12.
- ✓ **Nivel 4 – Anular habilidad mortífera**. Anula la habilidad más dañina del enemigo por todo el combate.

- Habilidades de la clase "Corpo":
  - ✓ **Nivel 1 – Acto de defensa.** Atrae el daño enemigo durante un turno.
  - ✓ **Nivel 2 – Puño de metal**. Golpea a un enemigo haciendo 1d6 y lo confunde completamente.
  - ✓ **Nivel 3 – Agarre bruto.** Agarra a un enemigo durante un turno, impidiendo que ataque y, además, recibirá cualquier ataque con toda seguridad.
  - ✓ **Nivel 4 – Embestida alocada.** Arremete contra un enemigo o un grupo de estos con toda su potencia física, provocando un daño de 1d12.
- Habilidades de la clase "Link":
  - ✓ **Nivel 1 – Compañero robot**. Convoca un dron que hace 1d4(tetraedro) de daño a un grupo de enemigos.
  - ✓ **Nivel 2 – Convencimiento pacífico**. Convence a un enemigo o un grupo de estos de no luchar si igual o supera 10 con 1d20 (icosaedro).
  - ✓ **Nivel 3 – Habla potenciadora**. Aumenta el daño de un aliado en su tirada en +3.
  - ✓ **Nivel 4 – Engaño audaz**. El mediador/a dará un discurso a un enemigo, diciéndole la conveniencia de actuar en favor del bien. Ayudará en la lucha contra el jefe con una acción única.
- Habilidades de la clase "Netrunner":
  - ✓ **Nivel 1 – Exploit.** Piratea cualquier dispositivo de seguridad si saca más de 10 tras usar el dado icosaedro.
  - ✓ **Nivel 2 – Firmware.** Modifica los parámetros de un grupo de enemigos, haciendo que su defensa baje a 5, lo cual facilita que reciban ataques de todo el grupo.

- ✓ **Nivel 3 – Echo.Off.** Se toman todos los dispositivos (no robots) del piso y se desactivan.
- ✓ **Nivel 4 – Banear habilidad.** Se anula una habilidad enemiga durante 3 turnos.

2. Sistema de juego

2.1. Sistema de acciones

Las acciones son las distintas tiradas que pueden realizarse con el objetivo de desbloquear una situación o un contenido previamente no disponible. Puede ser una conversación, un detalle de la historia, una función de una máquina… Todas estas acciones se realizan con el dado icosaedro (1d20). Todos los integrantes de los grupos deben tirar sus dados y luego sumar el resultado, y posteriormente se suma al del resto de grupos y se divide por el número de grupos cooperativos de la clase. De esta manera, se obtiene la media del resultado de todos los grupos en total. Según el resultado la acción saldrá según lo esperado o no.

- **"Investigación".** Esta acción tiene momentos obligatorios y puede usarse en cualquier sala en una ocasión para explorar número de enemigos o detalles de dicha habitación.
- **"Hacking".** Esta acción tiene momentos obligatorios y puede usarse en cualquier sala en una ocasión para piratear dispositivos de vigilancia u ordenadores para provocar distracciones, por ejemplo.
- **"Fuerza".** Esta acción tiene momentos obligatorios, y puede usarse en cualquier sala (una sola ocasión) para golpear un enemigo en distracción, lanzar objetos, romper algún objeto…
- **"Intimidación".** Esta acción no es obligatoria, pero puede usarse para obtener información de enemigos tras asustarlos.
- **"Persuasión".** Esta acción no es obligatoria, pero puede usarse para obtener información de enemigos tras convencerlos.
- **"Sigilo".** Esta acción no es obligatoria, pero puede usarse para saltarse un enfrentamiento o para hacer un ataque sorpresa.

2.2. Sistema de niveles

En esencia, existen 4 niveles, empezando todas las clases en el nivel 1 de partida. Al superar una corporativa se sube un nivel, adquiriendo con cada nivel una habilidad, un punto de subida de estadísticas (puede aplicarse a cualquiera de las seis) y se sube 1 punto de vida. Por tanto, al finalizar la corporativa Black ya se tienen las estadísticas, la vida y habilidades al máximo.

2.3. Sistema de combate

Este sistema funciona en gran sincronía con el sistema matemático de la actividad 13. Cada vez que se vaya a empezar un combate debe lanzarse un dado de 4, en función del resultado se hará un tipo de operaciones. Hecho esto, si toda la clase acierta el resultado y se retroalimentan de la forma correcta, comienza realmente el combate:

1- Al empezar se lanza un dado de 20 (1d20) por parte de cada "leader". Se dice la puntuación para decidir el orden de ataque. El docente actúa como los enemigos, por tanto, también lanza por su turno.
2- Posteriormente, se vuelve a lanzar, pero esta vez lo hacen todos los integrantes, debiendo superar el valor de la armadura del enemigo (el docente lo transmite) para poder acertar el ataque.
3- En caso de acertar, se lanza el dado de daño del arma disponible, y se levanta la mano al docente cuando pregunte: ¿Cuántos han hecho un daño de X? Así del 1-10 (el arma al mejor puede llegar a 10 de daño). De esta manera, el docente recopila rápidamente el daño y lo resta a los enemigos. Evidentemente, estos oponentes también atacan y deben acertar su ataque previamente (el docente conoce el valor de armadura).
4- Este proceso se repite hasta finalizar la vida de los enemigos. También pueden usarse habilidades, pero hay que recordar que gastan un punto de habilidad (6 puntos de habilidad para todo el gran grupo en cada corporativa, por tanto, debe decidirse previamente).

2.4. Sistema de avance

Este es el sistema más simple, ya que simplemente se basa en que con cada avance de piso o entrada a la sala de un jefe final deben acreditarse una serie de requisitos:

- Elaboración de una actividad al completo.
- Disposición de las suficientes medallas del juego.
- Disposición de un elemento específico del juego (solamente en la corporativa Black).

2.5. Sistema de logros y medallas

Las medallas del juego son llamadas "bitdatas". Esta es su forma:

Las medallas tienen la utilidad de permitir avanzar en la historia. Por otro lado, existe un sistema de logros que aporta más "bitdatas" de recompensa. Existirá un premio final si se consiguen todas las posibles:

- Logro 1. Derrotar 20 enemigos: 10 "bitdatas".
- Logro 2. Derrotar 50 enemigos: 30 "bitdatas".
- Logro 3. Derrotar al primer CEO: 10 "bitdatas".
- Logro 4. Derrotar al segundo CEO: 20 "bitdatas".
- Logro 5. Derrotar al tercer CEO: 30 "bitdatas".
- Logro 6. Derrotar al cuarto CEO: 40 "bitdatas".
- Logro 7. Derrotar al Tecnonauta: 100 "bitdatas".
- Logro 8. Conseguir todas las mejoras de arma: "50 bitdatas"
- Logro 9. Conseguir todas las mejoras de armadura: "50 bitdatas".
- Logro 10. Conseguir todas las "bitmedals" posibles. Se desbloquea una nueva historia que vivir a elección del alumnado. El docente la desarrollará al completo para trabajar otros contenidos.

3. Narrativa

3.1. Desarrollo de la historia

La misión se presenta en un vídeo: "Tenéis una misión: Salvad Exploit City". Este material audiovisual presenta al alumnado la necesidad de infiltrarse en cuatro corporativas con el objetivo de salvar la ciudad de un maléfico ciberdelincuente.

3.1.1. Corporativa Commons

Narración inicial: "En un inicio, está corporativa estaba dirigida por un comité de expertos en derechos de autor y licencias digitales. En esta época la empresa se encontraba en su mejor momento económico y todos sus trabajadores contaban con una buena posición dentro de la compañía. No obstante, ahora todo ha cambiado, ya que con la entrada del nuevo dirigente (el cual trabaja para el ciberdelincuente) toda la plantilla ha quedado reducida a robots. Pero esto no es nada comparado al cambio de ideales de la compañía, la cual está haciendo negocios asegurando protección y blindaje a recursos digitales con sus licencias, siendo una tapadera para luego alterarlas y vender las producciones al mejor postor.

Dicho esto, hay que decir que al contar con los planos de los últimos pisos de la corporativa Commons (punto en el que se localizan todos los activos y detalles clave de la empresa) la infiltración podrá correr menos riesgos. Suerte a todos y todas."

Piso 43

La primera barrera que puede encontrarse en este piso es su detector de directivos, ya que a partir de este punto solamente estos pueden acceder, exceptuando robots y androides. Para piratear este sistema debe usarse una tirada de "Hacking" y debe superarse la puntuación de 60 entre todos los dados. También puede usarse la habilidad "Ahora me perteneces" de la clase "Netrunner".

Habiendo superado este punto, el objetivo es llegar a las escaleras mecánicas situadas arriba a la izquierda, pero esto no será posible sin completar ciertas batallas y acciones a lo largo del piso (consiguiendo "bitdatas"). En cuanto se acceda a la primera a la sala, se encontrará una mesa a la izquierda, la cual está llena de robots hostiles (Enemigos: 6 robots RX-1). Una vez ganada la batalla, se conseguirán "bigdatas" suficientes para acceder al siguiente piso. Quedando dos opciones:

1- Acceder a la actividad 1, para la cual hacen falta 5 "bitmedals". Una vez acabada, puede accederse al siguiente piso. En dicho acceso hay dos cofres con 2 pociones de 1d6 (cada grupo obtiene los objetos, esto se mantiene en todos menos en las mejoras de armadura y armas).
2- Acceder a las otras habitaciones en las que hay dos píldoras narrativas (píldoras A y B) en los ordenadores. No obstante, hay dos enemigos custodiando dichas zonas (Enemigos: 2 robots RX-1 y 1 robot RX-2). Posteriormente, se accede a la actividad 1 con las "bitmedals", igual que en la primera opción.

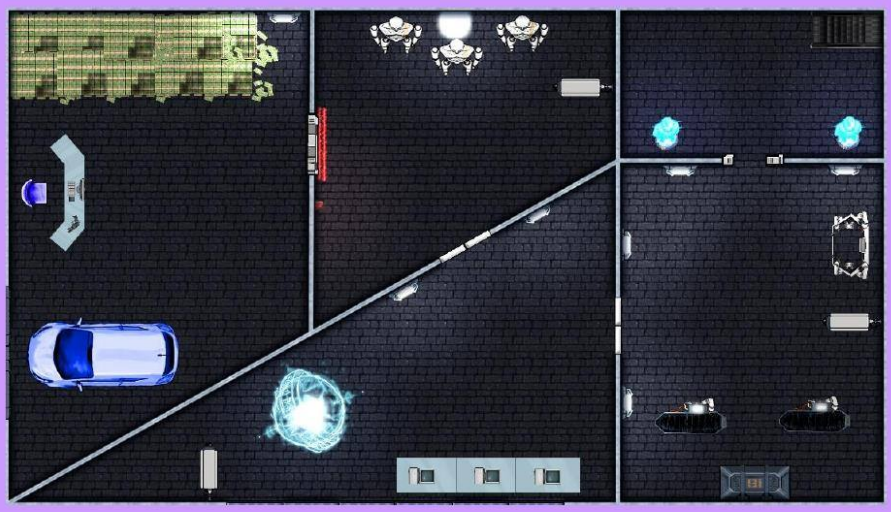
Piso 44

Al salir de la escalera se ve una puerta, tras ella hay dos trampas eléctricas que quitan a toda la clase 2 de vida, a no ser que se tire una tirada de "Investigación" y se supere la puntuación de 70. Tras salir de esta puerta, habrá unos robots (Enemigos: 3 robots RX-1). Este pasillo cuenta con una cámara, se tiene la opción de controlar dicho dispositivo con tirada de "Hacking" y se supere la puntuación de 80. En el caso de piratearla, los enemigos de habitaciones sucesivas no conocerán la posición de los héroes y heroínas, lo cual les permitirá una posición ventajosa (esto se extiende a todas las habitaciones que cuenten con cámara en el juego, no se repetirá esta información en ocasiones futuras). También está la opción de la habilidad de la clase "Netrunner". Tras avanzar por el pasillo y abrir la siguiente puerta, se verá un oficial robot destruido, si se lanza una tirada de "Investigación" que supere el valor de 90, se conseguirá averiguar una píldora narrativa (Píldora C). Por otro lado, en las habitaciones contiguas habrá un cofre con un dron táctico (permite ver una habitación sin entrar) y dos robots en unas cápsulas de hibernación (Enemigos: 2 robots RX-1).

En la siguiente habitación habrá tres robots y un oficial (Enemigos: 2 robots RX-2 y un robot X), los cuales custodian la entrada al siguiente piso. Tras el enfrentamiento, se debería contar con una cifra de 15 "bitdatas" para acceder a la actividad 2. Una vez finalizada, podrá verse un holograma del CEO de la corporativa Commons, Rachet Snovern. En dicho holograma, nos dejará el siguiente mensaje mientras aplaude: "Bravo,

sois la leche. Si habéis llegado hasta aquí significa que queréis morir a mis manos. Pronto le dejaré claro al Tecnonauta quién es el mejor CEO de los 4." Antes de acceder al siguiente piso, podrá verse un cofre a la izquierda con una mejora para el arma de toda la clase.

Piso 45



Tras subir las escaleras se llegará al último piso de la compañía. En la sala frontal se encontrará una zona de reparación de robots, en la cual habrá rivales duros de vencer (Enemigos: 2 robots RX-1 y 2 robots RX-3). El cofre de la habitación contendrá una bomba anulación (evita un turno de enemigos habituales). En cuanto se avance a la siguiente sala, se verá otro holograma de Snovern, esta vez dirá lo siguiente: "¿Sabéis cuánto me ha costado corromper esta compañía? Nada. Él me eligió, por eso no pienso perder. Si hay una manada de idiotas que quieren defender sus libritos y canciones, solamente podrán ser atendidos en la corporativa Commons, y después sus almas serán mías…JAJAJAJAJAJAJA"

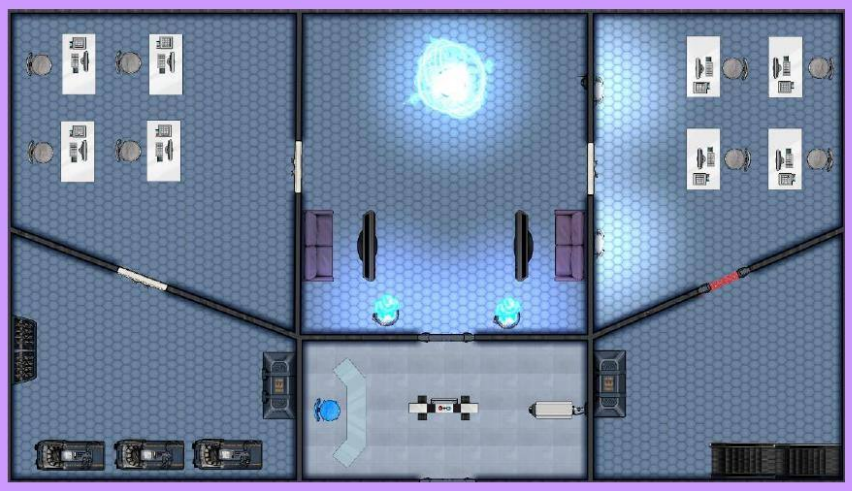
Tras salir de la habitación, por fin estará el acceso a la sala del jefe, serán necesarias 20 "bitdatas" para acceder a la actividad 3. Tras finalizar, comenzará la batalla con el CEO Snovern. Si cae derrotado, se accederá a una nueva píldora narrativa (Píldora D).

3.1.2. Corporativa Tegra

Narración inicial: "Esta empresa controla todos los medios de mensajería directa del mundo. Inicialmente se enorgullecía de que sus aplicaciones aseguraban una comunicación segura, en la cual no existía posibilidad de amenazar, acosar ni dañar a nadie. Al igual que en Commons, esta compañía tuvo un cambio de jefe, y supongo que podéis haceros una idea de qué ha ocurrido. Ahora la propia compañía contrata a una red de acosadores para dañar a personas alguna de sus aplicaciones. Justo después recibirán una oferta de otro software de mensajería, en el cual sus problemas desaparecerán. Pero claro, ¿a qué organización pertenecen todas las aplicaciones de mensajería? Sí, a la corporativa Tegra…

De nuevo, contáis con los planos de los últimos pisos de la corporativa Tegra. Os deseo suerte en la misión, la vais a necesitar."

Piso 38



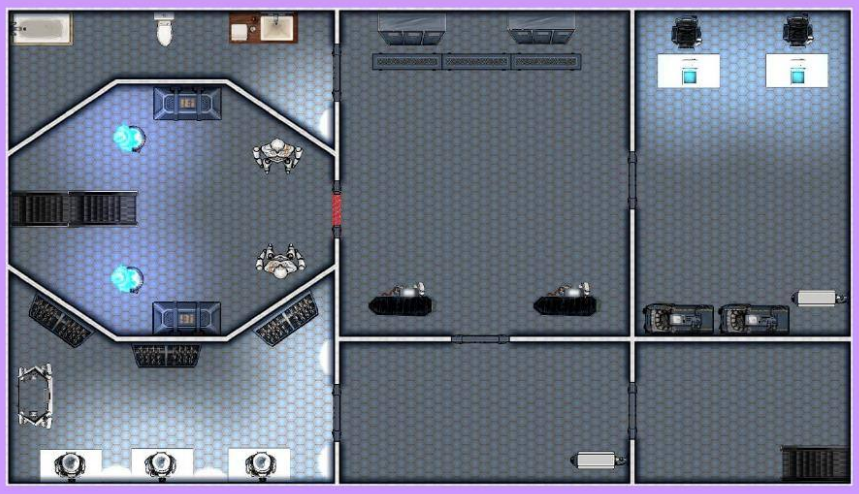
De nuevo, la entrada contará con sistemas de seguridad que habrá que piratear con las tiradas de "Hacking". Por suerte, el vigilante no está en su puesto. Al entrar, se podrá encontrar una sala de espera, en la cual habrá un holograma de la nueva CEO de la empresa, Ikumi Nakamura. En este caso el mensaje estará grabado: "Bienvenidos/as a la corporativa Tegra, si tienen una cita esperen pacientemente contemplando nuestras

ofertas en aplicaciones". En este caso, las puertas de la sala estarán cerradas a cal y canto, pero pueden destrozarse con una tirada de "Fuerza" siempre que se supere una puntuación de 70. Hay dos opciones:

1- La puerta de la izquierda lleva a una sala de trabajadores (Enemigos: 4 robots RX-4). Tras la batalla, podrá analizarse alguno de sus ordenadores con tirada de "Investigación", si se supera el 60 se descubrirá una píldora narrativa (Píldora E). Posteriormente, habrá una habitación con un cofre custodiado por un robot oficial (Enemigo: robot X). En dicho cofre habrá un dron táctico. Ahora puede recorrerse la vía de la puerta derecha.
2- La puerta de la derecha lleva a una sala de trabajadores (Enemigos: 4 robots RX-4). Tras la batalla, podrá analizarse alguno de sus ordenadores con tirada de "Investigación", si se supera el 90 se descubrirá una píldora narrativa (Píldora E). Tras esta sala se encuentra el acceso al siguiente piso. Para entrar se necesitan 25 "bitdatas", de esta forma se podrá comenzar la actividad 4. Si se desea, puede volverse hacia atrás para recorrer la puerta de la izquierda.

Antes de subir, podrá verse un cofre con una granada de impulso magnético (hace 1d4 de daño a un máximo de 4 enemigos).

Piso 39

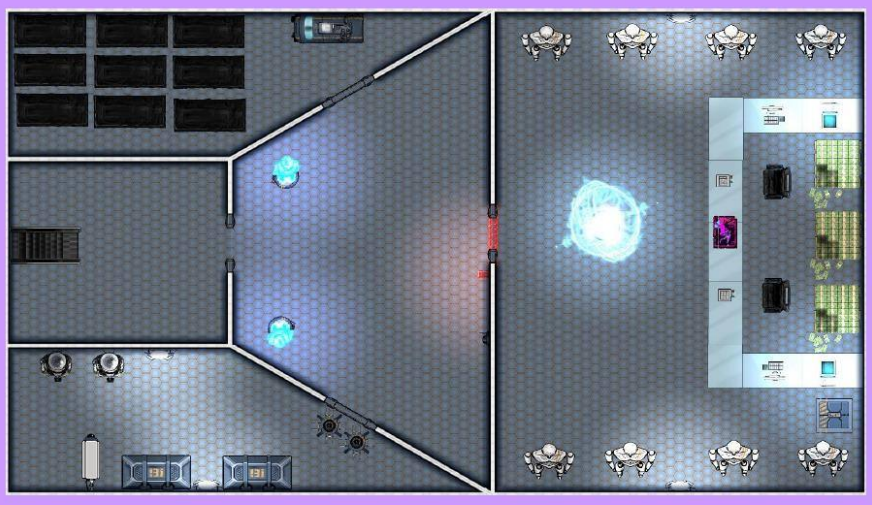


Tras haber llegado al siguiente piso, se podrá avanzar a un pasillo en el que de nuevo tenemos dos opciones:

1- La puerta frontal lleva a una zona con mejoras de armadura para las clases de "Leader", "Fixer" y "Corpo". Estarán custodiadas por dos poderosos adversarios (Enemigos: 2 robots RX-3). Luego puede regresarse al pasillo.
2- La puerta de la derecha conduce a una sala de reparaciones y recambios de robots, en ella habrá agentes no deseados (Enemigos: 4 robots RX-4). Justo a la izquierda está el acceso al siguiente nivel, para acceder a él se necesitan 40 "bitdatas". Así se desbloqueará la actividad 5 y se podrá seguir avanzando. No obstante, previamente hay otra puerta que lleva a una oficina con dos oficiales (Enemigos: 2 robots X). Esta sala contiene dos servidores, en los cuales puede lanzarse tirada de "Investigación". Si se supera la puntuación de 70 se desbloquea una nueva píldora (Píldora F).

Antes de las escaleras habrá dos cofres a izquierda y derecha, ambos contienen dos pociones de 1d8.

Piso 40



El último piso de la corporativa Tegra está al subir los peldaños. Habiendo llegado, se puede ver una sala frontal con algunos malos de turno (Enemigos: 4 robots RX-1). Dicha sala tiene tres puertas, siendo una de ellas (puerta central) la sala del jefe final. Para ella

hacen falta 50 "bitdatas", desbloqueando a su vez la actividad 6. No obstante, merece la pena contemplar las otras dos puertas:

1- La puerta a la izquierda lleva a una sala defendida por un oficial (Enemigo: robot X). Si se lanza una tirada de "Investigación" y se supera el valor de 70 se encontrará la píldora correspondiente (Píldora G).
2- La puerta a la derecha da a una sala con dos cofres (contienen un dron táctico y una mejora de arma) y las últimas dos mejoras de armadura (clases "Link" y "Netrunner"). Dicha habitación tiene habitantes malignos (Enemigos: 3 robots RX-2) y habrá que vencerlos.

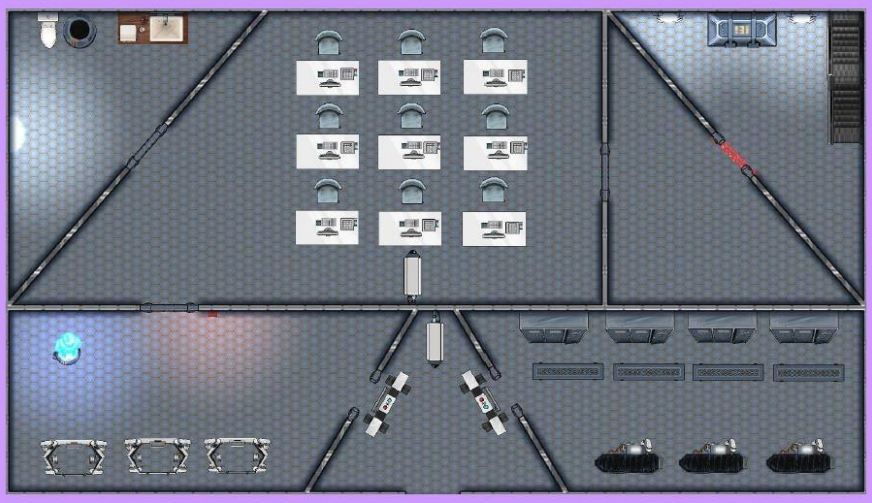
Cuando se penetre la sala del jefe final, se verá a una mujer japonesa hablando con un "cyborg" al que no se le puede ver la cara. Solamente se escuchará este último mensaje: "Tranquilo Tecnonauta, me encargaré de ellos y ellas personalmente. Serán pasto de mi modo clon." Tras soltar esa última frase, el holograma desaparecerá e Ikumi Nakamura se dirigirá a los héroes y heroínas con la siguiente afirmación: "¿No podíais quedaros tranquilitos y tranquilitas en la sala de espera? Tenía una gran sorpresa reservada con mi gas neutralizador. Es igual, habéis insistido en comunicaros conmigo por mensajería directa. Pues genial, mensaje leído con doble marca azul. Me encargaré de acosaros físicamente personalmente". En ese momento aparece otra Ikumi Nakamura sentada en el otro sillón vacío disponible. Eso marcaría el inicio de la gran batalla. Si se derrota a la CEO de la Corporativa Tegra, se podrá acceder a un cartel que está sobre la mesa. Este será la siguiente píldora narrativa (Píldora H).

3.1.3. Corporativa Black

Narración inicial: "En el pasado, esta compañía se encargaba del diseño de los sistemas de ciberseguridad de todas las casas, empresas y gobiernos del mundo. Ahora digamos que solamente se encargan de cesar con sus propios ciberataques y virus si hay una transferencia con muchos ceros. Atacar y destruir para luego defender y reconstruir, en esa es la estrategia de la Corporativa Black desde que su nueva CEO está al frente. Pero lo peor está por llegar, la idea es infiltrarse y acabar con unos expertos en atacar digitalmente. Pues mucha suerte…

Los planos de esta empresa han costado la vida de dos buenos "netrunners" de Exploit City. Solo espero que merezca la pena por sus sacrificios."

Piso 63

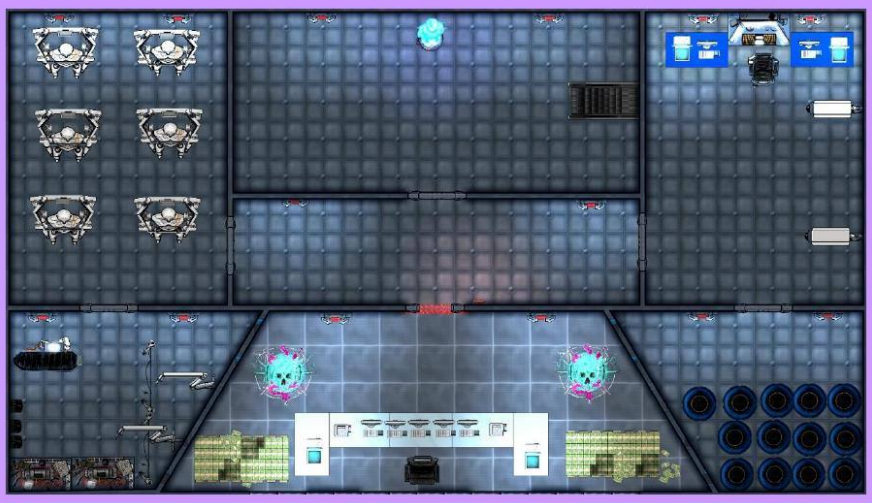


El primer piso contiene una nueva sala de seguridad, para superarla debe seguirse el procedimiento habitual, tomar la opción de tirar "Hacking" u optar por las habilidades de la clase "Netrunner". Si se va hacia a la izquierda, se encontrará una puerta con un sistema de lectura de tarjeta de empleado. Dicho sistema pone lo siguiente: "Tarjeta de acceso de nivel 1". Al no disponerse de dicha tarjeta, se tendrá que revisar en la otra habitación disponible. Esta sala es un vestuario de robots, en el cual habrá que lanzar tirada de "Investigación", si se supera el valor de 50 se localizará una tarjeta de empleado bajo la taquilla situada más a la derecha. Con ella, al fin se podrá entrar en la primera oficina de trabajo, la cual está repleta de trabajadores hostiles (Enemigos: 9 robots RX-1). Una vez derrotados, solamente se dará relevancia a la zona de la derecha, ya que la otra parte es un baño. Al pasar la puerta, dos tartanas robóticas (Enemigos: 2 robots RX-3) darán la bienvenida a los visitantes. Justo detrás de ellos se encuentra el acceso al siguiente piso, y se podrá avanzar con 60 "bitdatas", pero antes habrá que hacer la actividad 7. Al lado de las escaleras habrá un cofre con una granada de impulso magnético. Ahora toca ascender sin demora.

Piso 64

Lo primero que se puede ver es una puerta de acceso con tarjeta de empleado de nivel 1. Evidentemente, se podrá avanzar, ya que se cuenta con él. Posteriormente se verá un oficial (Enemigo: robot X) con una tarjeta de nivel 2 sobre la mesa. El objetivo es simple, derrotarlo y obtenerla. Una vez hecho esto, se podrá acceder a la siguiente sala y habrá que repetir la misma operación y obtener una de nivel 3. En la siguiente sala ocurrirá exactamente lo mismo, pero con el nivel 4. Debe decirse que, si se ha estado atento a las televisiones de las salas de cada oficial, se podrá ver un número en cada una. Todos eso números formarán la contraseña de ordenador del oficial de más alto rango, y en el caso de acceder se podrá ver la primera píldora narrativa de esta corporativa (Píldora I). De esta manera, se finaliza la andadura por las salas de oficiales, llegando a una sala con un alijo que contiene una mejora para armas y una poción de 1d8. Justo al lado está el acceso al siguiente piso. Para pasar se necesitan 70 “bitdatas” y superar la actividad 8. Luego solamente queda subir las escaleras.

Piso 65



El último piso presenta la puerta de la CEO casi al principio, pero esta tiene unas características curiosas. En este caso para entrar no solamente hacen falta "bitdatas" (en este caso 80), sino que también hace falta una tarjeta de nivel 6. El pasillo tiene dos vías:

1- Hacia la izquierda se llega a las estancias de uno de los máximos directivos, el cual se hace llamar "El virólogo" (Enemigo: robot X-2). Si se sigue por ese sentido, se llegará hasta él y comenzará un combate en su sala de pruebas con virus y tecnología. Allí, se conseguirá una tarjeta con banda, pero no es de nivel 6, simplemente no tiene ningún nivel.
2- Hacia la derecha se llega a la sala de vigilancia, en la cual se encuentra su vigía (Enemigo: robot RX-3). En esta sala se puede encontrar una especie de datáfono con un número 6 metalizado. Quizás si se pasa alguna tarjeta puede tener alguna utilidad. En la parte trasera hay un pequeño almacén con recipientes llenos de USB 20.0 con virus troyanos y gusanos.

No importa qué camino se tome, ya que habrá que recorrer ambos para formar la tarjeta de nivel 6. Una vez hecho esto, ya se podrá pasar y afrontar la actividad 9. Tras cruzar la puerta, estará esperando Heather Firewall, la nueva CEO de la corporativa Black. Como es lógico pensar, tiene un discurso que dar a sus huéspedes: "Vaya, vaya, vaya…Aquí

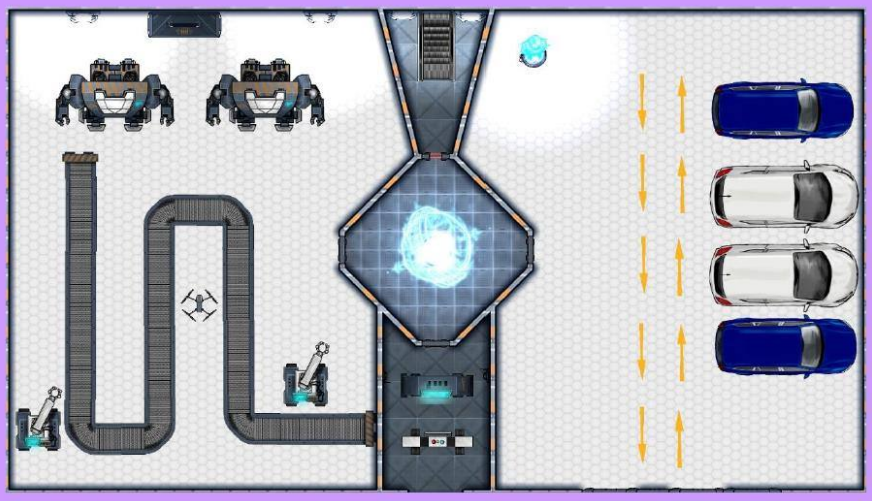
están los frikis que derrotaron a Nakamura y Snovern. Pues sinceramente no parecéis muy fuertes, pero ya veremos qué tenéis que decir ante eso. El Tecnonauta me ha avisado correctamente de vuestra llegada, por eso vamos a jugar a un juego mortal, el cual termina con vuestros cerebros llenos de nanotecnología y yo haciendo uso de ellos. Tranquilos y tranquilas, morir es como un error 404, pero viéndolo todo el tiempo en bucle. JAJAJAJAJAJAJAJAJA". Con el final de la risa la batalla comienza…Si los grupos de héroes y heroínas vencen conseguirán una píldora narrativa (Píldora J).

3.1.4. Corporativa Likers

Narración inicial: "Hace dos siglos, todas las redes sociales estaban separadas con sus distintas funcionalidades. Con el tiempo, surgió una compañía que las adquirió todas para transformarlas en una que unificara todas las características y funciones. Actualmente, en el siglo XXIII, dicha empresa sigue siendo la dueña de la única red social existente. Esta no es otra que la corporativa Likers. Imaginad lo que puede ocurrir si esta red cae en las manos equivocadas, sin duda, podría ser toda una catástrofe de vulneración y evasión de los derechos de las personas. Pues la realidad es aún peor, ya que la nueva CEO de la compañía adquiere datos personales con el objetivo de controlar a todos los usuarios. Evidentemente, la empresaria sabe lo que ha ocurrido con las otras tres corporativas. Por ello, no esperéis una cálida bienvenida. Toda la corporativa estará preparada para la infiltración. Pero no importa, es la hora de acabar con esto y conseguir que el Tecnonauta salga a la luz.

Tomad los planos de la empresa. Id y restaurad la antigua gloria de Exploit City. Antes la esperanza solo era un anhelo, pero ahora…Ahora todos creemos en vosotros y vosotras".

Piso 81



El primer piso tiene una sala de seguridad con un escáner biométrico de movimiento (además en esta corporativa ya no se usan cámaras, ahora se emplean drones). Para avanzar esta zona se tendrá que lanzar una tirada de "Hacking" que supere 90, de lo contrario se contará con dos enemigos poderosos de más. Una vez se avance a la siguiente sala, se encontrará un holograma de la CEO, Trinity Finenn. En el encuentro dirá lo siguiente: "Tal y como esperaba, al fin estáis aquí. El Tecnonauta quedará encantado cuando os aplasten los nuevos robots que he creado. Pero todavía será mejor cuando saquemos capturas del momento. Ya imagino la repercusión de mis publicaciones…Seré viral hasta el fin de mis días. JAJAJAJAJAJAJAJA". Con esto acaba el mensaje y el holograma se desactiva. Hay tres puertas, estando una en el centro, otra en la izquierda y otra en la derecha de la sala:

1- La puerta de la derecha lleva a los coches voladores, situados en un garaje que da al exterior del edificio.
2- La puerta de la izquierda lleva a una fábrica de robots especiales. Los operarios son poco amigables, como era de esperar (Enemigos: 6 robots RX-4). Por otro lado, si el sistema de defensa se activó también habrá dos robots X-3 activos. En el cofre del fondo hay una bomba de impulso magnético.

3- La puerta central conduce al siguiente piso y se necesitan 90 “bitdatas” para atravesar el umbral y, por tanto, poder realizar la actividad 10.

Piso 82

Tras salir por la puerta frente a la escalera, se podrá ver dos cofres situados a la izquierda, los cuales contienen dos pociones de 1d8. No obstante, desde que se tomen dichos ítems habrá una emboscada terrible (Enemigos: 2 robots X-3). Si se sobrevive al ataque, se podrá atravesar la puerta a una oficina en la que hay trabajadores concentrados (Enemigos: 6 robots RX-1). En la sala contigua habrá otro gigante esperando (Enemigo: robot X-3), el cual cubre la entrada al último piso. En este punto ya habría que tener 110 “bitdatas” para avanzar a la actividad 11. Una vez hecha, será tiempo de adentrarse en el último piso. Si se quiere reflexionar o planear algo es el momento.

Piso 84

Ya en el piso final, por un lado, podrá verse la última mejora de armadura para todas las clases y, por otro lado, los cofres contendrán la última mejora de las armas y un revivir grupal (revive a 5 personas a la vez). La puerta para ir a la oficina del jefe final solamente necesitará de la realización de la actividad 12. Una vez se termine con la actividad, ya no hay vuelta atrás, será el momento de luchar. La batalla comenzará con tres duros oponentes (Enemigos: 3 robots X-3), mientras Finenn nos observará detenidamente. Al derrotar a sus esbirros, dirá los siguiente: "Mi señor, tan solo vedme, ser viral está ahora a mi alcance". Justo después comenzará la batalla contra la última CEO. En caso de victoria se manifestará el Tecnonauta, pero… ¿Quién es? No es otra persona que el docente que ha diseñado todo esto, un vil traidor que se ha hecho inmortal en las redes usándolas en su beneficio desde el siglo XXI. El Tecnonauta es Alejandro Dayekh García.

"Ahora es mi momento de hablar, durante todo este tiempo yo he guiado esta historia para formar vuestras habilidades en la red. Seguramente ahora pensáis que podéis protegeros de las amenazas de internet. Todo este tiempo os habéis hecho una idea equívoca, yo soy el Tecnonauta, os he hecho sentir seguros y vivir una historia en la que sois héroes y heroínas, pero en realidad bailabais en la palma de mi mano. Todos y todas pensabais que la amenaza era la propia red, pero el mayor peligro siempre fui yo. Uníos

a mí como mis nuevos directivos de las compañías y tomad el mundo para mí. Uníos a mí o simplemente…Suspended". Comienza la batalla final.

La victoria en este enfrentamiento significará el final de la historia. Exploit City habrá sido liberada de la tiranía del Tecnonauta.

3.1.5. Píldoras narrativas

- ***Píldora A***. Un contrato laboral firmado por el nuevo CEO: su nombre es Rachet Snovern. En dicho papel oficial se ve que paga a sus trabajadores y trabajadoras un plus por cada documento que se desvía de forma exitosa, vulnerando las licencias.
- ***Píldora B***. Un email firmado por el Tecnonauta a Rachet Snovern. En ella solo hay escrito lo siguiente: "Ten cuidado, asegúrate de arreglar al oficial robot de la segunda planta que defiende el acceso a tu piso".
- ***Píldora C***. El antiguo oficial de la empresa. Su nombre era Müller Howkings. Trabajó para el nuevo CEO durante un mes, hasta que se reveló por las actividades corruptas de su nuevo jefe y robó la siguiente información: "Al parecer Snovern cuenta con una pistola de rayos con la que falla tiros a propósito, ya que luego rebotan y te atacan en otro momento."
- ***Píldora D***. Un documento digital del Tecnonauta. En el apartado de firma las siglas escritas son: G. D. A.
- ***Píldora E***. Los ordenadores contienen conversaciones en las que se ve que los trabajadores están insultando, acosando y chantajeando a distintas personas por servicios de mensajería.
- ***Píldora F.*** En una carpeta codificada hay dos datos de la CEO: "Ikumi Nakamura" (nombre) y "Duplicación" (habilidad).
- ***Píldora G***. Bajo las lonas se ocultan robots destruidos que se arrepintieron de acosar y maltratar a personas en las aplicaciones. Todo ello solamente con el objetivo de derivarlas a otras mensajerías que son promocionadas como seguras por otros empleados.
- ***Píldora H.*** Un cartel de posesión del Tecnonauta, pero es extraño. Parece bastante antiguo para el siglo XXIII.

- ***Píldora I.*** Tras poner la contraseña, se podrá ver los datos de un robot. Su modelo es X-2 y tiene una fuerza descomunal, ya que es capaz de hacer un golpe de 1d10 de daño a 10 enemigos a la vez. Sin embargo, al parecer este robot es muy sociable, quizás se le pueda persuadir…
- ***Píldora J***. El Tecnonauta escribe lo siguiente a Heather: "Si quieres crear el virus definitivo mantén mi secreto. Si ellos y ellas se enteran todo mi plan se irá al traste. No pueden saber que ya me han visto en Exploit City".

3.2. Enemigos de la historia

3.2.1. Jefes finales

CEO Rachet Snovern (PV: 150 / Armadura 12)

- **Arma.** Pistola de rayos rebotadores:
  - Daño único. (1d6). Siempre golpea un turno después.
  - Ataque combinado. (5d4) Dispara 5 disparos al mismo tiempo.
- **Habilidades**
  - Rayo en área. (1d4) Golpea a 5 personas el mismo daño.

CEO Ikumi Nakamura (PV: 150/ Armadura 13)

- **Arma.** Látigo de descargas eléctricas:
  - Ataque combinado. (1d6) Ataca a 10 a la vez.
- **Habilidades**
  - Duplicación. Dos Ikumi atacan a la vez todos los ataques.

CEO Heather Firewall (PV: 200 / Armadura 13)

- **Arma.** Arma psíquica de virus:
  - Daño único. (1d8). Concentra un ataque mental que anula un turno.
  - Ataque combinado. (3d6) Ataque a 3 personas distintas.
- **Habilidades**
  - Control mental. Controla las acciones de un aliado por 3 turnos.

CEO Trinity Finenn (PV: 250 / Armadura 14)

- **Arma.** Concentrador de plasma:
  - Daño único. (1d10). Concentra un ataque de plasma.
  - Daño combinado. (3d12). Concentra tres ataques durante un turno.
- **Habilidades**
  - Like. La armadura aumenta en 5 durante 1 turno.

Tecnonauta: Alejandro Dayekh García (PV 300 / Armadura 14)

- **Arma:** Brazo Cyborg:
  - Daño único. (1d12). Ataca con su puño a máxima velocidad.
  - Daño combinado. (5d12). Realiza una onda de choque a 5 objetivos.
- **Habilidades:**
  - Suspenso general. Elimina un turno a todos.

3.2.2. Enemigos habituales

Robot RX-1 (PV: 30 / Armadura 9)

Daño. 1d6.

Bitdatas de recompensa: 1

Robot RX-2 (PV: 50 / Armadura 10)

Daño. 1d6.

Bitdatas de recompensa: 3

Robot RX-3 (PV: 60 / Armadura 11)

Daño. 1d8.

Bitdatas de recompensa: 5

Robot RX-4 (PV: 80 / Armadura 11)

Daño. 1d8.

Bitdatas de recompensa: 10

Robot X (PV: 100 / Armadura 12)

Daño. 1d8.

Bitdatas de recompensa: 15

Robot X-2 (PV: 150 / Armadura 8)

Daño. 1d8. (1d10 a 10 personas en momentos de tensión)

Bitdatas de recompensa: 15

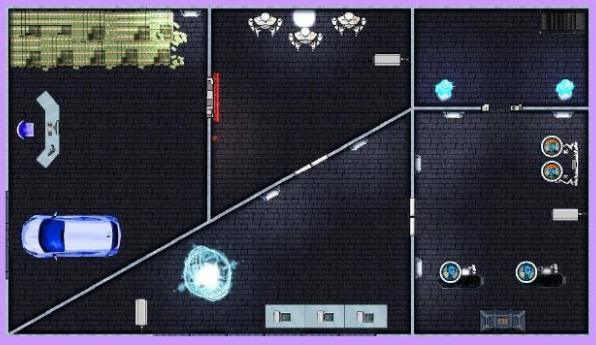
Robot X-3 (PV: 150 / Armadura 12)

Daño. 1d10.

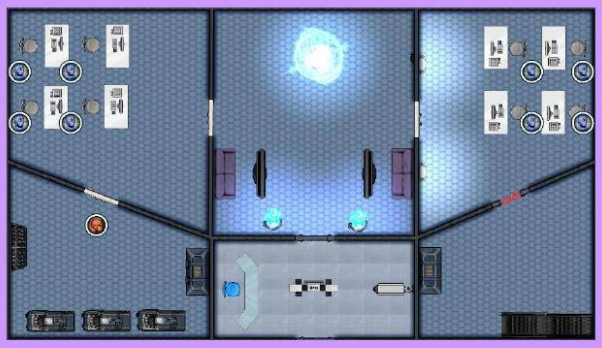
Bitdatas de recompensa: 20

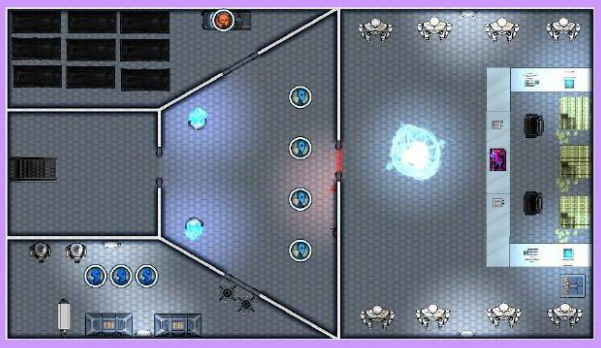
3.2.3. Posición de los enemigos

- Corporativa Commons

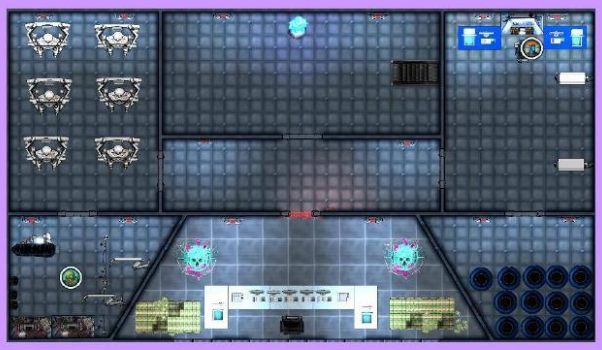


- Corporativa Tegra





- Corporativa Black



- Corporativa Likers

Anexo Q. Recursos digitales de la gamificación “Exploit City”

En este punto de anexos se aportan los recursos para su descarga. Todos los recursos contienen la licencia CC BY – NC – SA 4.0.

- Manual de la gamificación “Exploit City”: Descarga
- Imágenes de los enemigos: Descarga
- Imágenes de los mapas: Descarga
- Logo de la gamificación: Descarga
- Presentación de la misión: Enlace
- Web de presentación: Enlace

Anexo R. Recursos digitales de la valoración

En este punto de anexos se aportan los cuestionarios para su descarga.

- Formulario de valoración sin cumplimentar (Docente): Descarga
- Formulario de valoración sin cumplimentar (Policía): Descarga

Anexo S. Respuesta de formulario de valoración (Policía)

Formulario de valoración "Exploit City" (Policía)

Bienvenido/a, antes de comenzar el cuestionario le comunicaré una serie de cuestiones:

1 - Todos los datos que usted ponga en el cuestionario se usarán para fines académicos. Por tanto, solamente son un aval de que esta valoración está acreditada por los expertos o expertas correspondientes. En ningún caso se hará un uso distinto de ellos. De hecho, todos ellos quedarán reflejados en un repositorio institucional (https://reunir.unir.net/), el cual cuenta con licencia CC BY - NC - ND, garantizando la seguridad de que estos datos no tendrán otro tipo de uso que la divulgación educativa/académica.

2 - Todas las respuestas son tomadas como valiosas, por tanto, si desea establecer ideas críticas solamente podrá beneficiar a la mejora del proyecto. Su sinceridad es primordial.

3 - Mi agradecimiento total por ayudar a completar este Trabajo de Fin de Máster con la visión experta de las Fuerzas de Seguridad del Estado.

Dicho esto, conteste con calma las preguntas, ya que no son demasiadas. Adelante...

Nombre (NOMBRE, NO APELLIDOS) del Policía Local / Nacional *

Roberto.

Número de placa u otro dato que acredite la condición de policía *

102156

Provincia *

Santa Cruz de Tenerife

Como policía: ¿Cree que la temática del proyecto (Introducción de conductas de ciberseguridad) es adecuada para trabajar en edades de entre 11-12 años? *

- (●) Sí, ya que en estas edades ya hay un uso importante de tecnología e internet
- ( ) No, ya que en estas edades aún no hay un uso importante de tecnología e internet
- ( ) Ns / Nc.

Como policía: ¿Considera conveniente que la escuela incluya contenidos y aspectos curriculares sobre ciberseguridad para la educación de los menores? *

- (●) Sí, considero necesario que se ahonde en el dilema con actividades y proyectos.
- ( ) No, considero que el papel de agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc.) ya es suficiente.
- ( ) No, considero que son las familias quiénes deben afrontar esta realidad por su cuenta.
- ( ) Ns / Nc.

Como policía: ¿Piensa que "Exploit City" puede ser un proyecto útil para la introducción de estos contenidos en el aula? Tenga en cuenta la respuesta que dio en la pregunta anterior. *

- ( ) Sí. este es un buen ejemplo de desarrollo de conductas seguras en la red para menores.
- ( ) No, considero que este proyecto no es capaz de afrontar correctamente este dilema.
- (●) Tal vez, siempre que hayan profesionales externos que se aseguren de la validez y solidez de la propuesta.
- ( ) Ns / Nc.

Como policía: ¿Comparte la visión de que el público adolescente puede resistirse al aprendizaje de conductas seguras en la red, siendo necesarias metodologías que "motiven" y "diviertan" a los menores? *

- (●) Sí, los niños y niñas deben sentirse cómodos al tratar estos temas que atañen a su libertad.
- ( ) No, los niños y niñas deben obtener esos aprendizajes por imposición adulta.
- ( ) Tal vez, mientras los menores no obtengan un aprendizaje equívoco de dichas conductas seguras.
- ( ) Ns / Nc.

Como policía: ¿Considera que la evasión de los derechos de autor / licencias digitales es un problema que puede corregirse en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, dotar a los menores del respeto a la propiedad intelectual evitará posibles delitos futuros en esta temática.
- ( ) No, ya que este tema es demasiado complejo como para trabajarlo en estas franjas de edad.
- ( ) Ns / Nc.

Como policía: Habiendo visto las actividades de la Corporativa Commons (fase 1), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- ( ) Sí, estas actividades pueden ser un buen método de trabajo de las licencias y derechos de autoría.
- ( ) No, ya que esto puede superar lo que los pequeños y pequeñas pueden comprender.
- (●) Tal vez, todo depende de la calidad del diseño de esas actividades y de la formación del docente.
- ( ) Ns / Nc.

Como policía: ¿Considera que el ciberacoso es un problema que debe ser abordado en edades escolares de Educación Primaria (11 - 12 años)? *

- ○ Sí, estas edades son especialmente críticas en estos delitos virtuales.
- ○ No, ya que estos delitos deben ser trabajados en edades de secundaria (E.S.O / Bachiller).
- ◉ Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ○ Ns / Nc.

Como policía: Habiendo visto las actividades de la Corporativa Tegra (fase 2), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- ◉ Sí, estas actividades pueden ser una buena alternativa para conocer los peligros de cada tipo de ciberacoso y distintos sistemas de defensa ante ellos.
- ○ No, estas actividades no ayudarán a solucionar el problema del ciberacoso o a mejorar el conocimiento sobre el mismo.
- ○ Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ○ Ns / Nc.

Como policía: ¿Considera que el malware o los programas malignos pueden ser abordados en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, ya que el aumento de delitos cibernéticos afecta a toda la sociedad y, por tanto, una concienciación temprana es necesaria.
- ( ) No, estos programas fraudulentos y peligros no pueden ser usados en ningún contexto en educación.
- ( ) Tal vez, siempre y cuando el contexto sea conveniente y seguro.
- ( ) Ns / Nc.

Como policía: Habiendo visto las actividades de la Corporativa Black (fase 3), ¿cree que pueden ser una forma correcta de conocer el malware? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, ya que conocer bien el funcionamiento y la composición de los virus puede ayudar a evitarlos correctamente.
- ( ) No, lo conveniente es no abordar este dilema tecnológico en la escuela.
- ( ) Tal vez, siempre y cuando solamente sean métodos pasivos (antivirus, programas, etc.), dejando de lado métodos manuales para investigar.
- ( ) Ns / Nc

Como policía: ¿Considera que las redes sociales y su funcionamiento pueden ser abordados en edades escolares de Educación Primaria (11-12 años)? *

- (●) Sí, en estas edades el uso de redes sociales se dispara y no se conocen los riesgos ni condiciones de uso.
- ( ) No, las redes sociales deben evitarse lo máximo posible, eliminándolas de la realidad del menor. Por ello, no deben introducirse en ninguna clase.
- ( ) Tal vez, siempre que se usen en momentos puntuales con un objetivo claro.
- ( ) Ns / Nc.

Como policía: Habiendo visto las actividades de la Corporativa Likers (fase 4), ¿cree que pueden ser una manera idónea de introducir al uso adecuado de las redes sociales y sus características? *

- (●) Sí, las actividades dan una visión bastante amplia de los detalles únicos de cada red social, aumentado la probabilidad de un buen uso futuro.
- ( ) No, es conveniente apartar estos mecanismos de contacto social alejados del menor.
- ( ) Tal vez, siempre que haya un control extremo de su uso, sin dejar margen de exploración.
- ( ) Ns / Nc.

Como policía: ¿Cree que este proyecto puede ayudar a reducir el número de delitos relacionados con ciberdelincuencia? *

- (●) Sí.
- ( ) No.
- ( ) Tal vez.
- ( ) Ns / Nc.

Como policía: ¿Cree que este proyecto puede ayudar a aumentar el número de denuncias de este tipo de delitos digitales, los cuales suelen pasar desapercibidos? *

- ( ) Sí.
- ( ) No.
- (●) Tal vez.
- ( ) Ns / Nc.

Como policía: ¿Cree que este proyecto puede garantizar unas conductas y competencias en la red que mantengan a los menores protegidos dentro de sus márgenes de libertad online? *

- (●) Sí.
- ( ) No.
- ( ) Tal vez.
- ( ) Ns / Nc.

Para finalizar puede añadir sugerencias, comentarios o mejoras al autor del proyecto: *

Como profesional ...he visto que la presentación del proyecto esta muy bien y considero que la clave para lograr el objetivo primordial del mismo de conseguir una educación integral en cuanto al uso de las nuevas tecnologías..en esta era digital es fundamental si inclusión en la educación, es una paridad de profesionales del mundo educativo, informático y de las fuerzas y cuerpos de seguridad.

Anexo T. Respuestas del formulario de valoración (Docentes)

Formulario de valoración "Exploit City" (Docente)

Bienvenido/a, antes de comenzar el cuestionario le comunicaré una serie de cuestiones:

1 - Todos los datos que usted ponga en el cuestionario se usarán para fines académicos. Por tanto, solamente son un aval de que esta valoración está acreditada por los expertos o expertas correspondientes. En ningún caso se hará un uso distinto de ellos.

2 - Todas las respuestas son tomadas como valiosas, por tanto, si desea establecer ideas críticas solamente podrá beneficiar a la mejora del proyecto. Su sinceridad es primordial.

3 - Mi agradecimiento total por ayudar a completar este Trabajo de Fin de Máster con la visión experta de docentes en activo.

Dicho esto, conteste con calma las preguntas, ya que no son demasiadas. Adelante...

Nombre del docente (SOLO NOMBRE) *

Santiago

Ámbito de docencia *

Educación Primaria

Institución educativa *

Colegio Máyex

Como docente: ¿Cree que la temática del proyecto (Introducción de conductas de ciberseguridad) es adecuada para trabajar en edades de entre 11-12 años? *

- (●) Sí, ya que en estas edades ya hay un uso importante de tecnología e internet
- ( ) No, ya que en estas edades aún no hay un uso importante de tecnología e internet
- ( ) Ns / Nc.

Como docente: ¿Considera conveniente que la escuela incluya contenidos y aspectos curriculares sobre ciberseguridad para la educación de los menores? *

- (●) Sí, considero necesario que se ahonde en el dilema con actividades y proyectos.
- ( ) No, considero que el papel de agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc.) ya es suficiente.
- ( ) No, considero que son las familias quiénes deben afrontar esta realidad por su cuenta.
- ( ) Ns / Nc.

Como docente: ¿Piensa que "Exploit City" puede ser un proyecto útil para la introducción de estos contenidos en el aula? Tenga en cuenta la respuesta que dio en la pregunta anterior. *

- (●) Sí. este es un buen ejemplo de desarrollo de conductas seguras en la red para menores.
- ( ) No, considero que este proyecto no es capaz de afrontar correctamente este dilema.
- ( ) Tal vez, siempre que hayan profesionales externos que se aseguren de la validez y solidez de la propuesta.
- ( ) Ns / Nc.

Como docente: ¿Comparte la visión de que el público adolescente puede resistirse al aprendizaje de conductas seguras en la red, siendo necesarias metodologías que "motiven" y "diviertan" a los menores? *

- (●) Sí, los niños y niñas deben sentirse cómodos al tratar estos temas que atañen a su libertad.
- ( ) No, los niños y niñas deben obtener esos aprendizajes por imposición adulta.
- ( ) Tal vez, mientras los menores no obtengan un aprendizaje equívoco de dichas conductas seguras.
- ( ) Ns / Nc.

Como docente: ¿Considera que la evasión de los derechos de autor / licencias digitales es un problema que puede corregirse en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, dotar a los menores del respeto a la propiedad intelectual evitará posibles delitos futuros en esta temática.
- ( ) No, ya que este tema es demasiado complejo como para trabajarlo en estas franjas de edad.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Commons (fase 1), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, estas actividades pueden ser un buen método de trabajo de las licencias y derechos de autoría.
- ( ) No, ya que esto puede superar lo que los pequeños y pequeñas pueden comprender.
- ( ) Tal vez, todo depende de la calidad del diseño de esas actividades y de la formación del docente.
- ( ) Ns / Nc.

Como docente: ¿Considera que el ciberacoso es un problema que debe ser abordado en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, estas edades son especialmente críticas en estos delitos virtuales.
- ( ) No, ya que estos delitos deben ser trabajados en edades de secundaria (E.S.O / Bachiller).
- ( ) Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Tegra (fase 2), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, estas actividades pueden ser una buena alternativa para conocer los peligros de cada tipo de ciberacoso y distintos sistemas de defensa ante ellos.
- ( ) No, estas actividades no ayudarán a solucionar el problema del ciberacoso o a mejorar el conocimiento sobre el mismo.
- ( ) Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ( ) Ns / Nc.

Como docente: ¿Considera que el malware o los programas malignos pueden ser abordados en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, ya que el aumento de delitos cibernéticos afecta a toda la sociedad y, por tanto, una concienciación temprana es necesaria.
- ( ) No, estos programas fraudulentos y peligros no pueden ser usados en ningún contexto en educación.
- ( ) Tal vez, siempre y cuando el contexto sea conveniente y seguro.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Black (fase 3), ¿cree que pueden ser una forma correcta de conocer el malware? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, ya que conocer bien el funcionamiento y la composición de los virus puede ayudar a evitarlos correctamente.
- ( ) No, lo conveniente es no abordar este dilema tecnológico en la escuela.
- ( ) Tal vez, siempre y cuando solamente sean métodos pasivos (antivirus, programas, etc.), dejando de lado métodos manuales para investigar.
- ( ) Ns / Nc

Como docente: ¿Considera que las redes sociales y su funcionamiento pueden ser abordados en edades escolares de Educación Primaria (11-12 años)? *

- (●) Sí, en estas edades el uso de redes sociales se dispara y no se conocen los riesgos ni condiciones de uso.
- ( ) No, las redes sociales deben evitarse lo máximo posible, eliminándolas de la realidad del menor. Por ello, no deben introducirse en ninguna clase.
- ( ) Tal vez, siempre que se usen en momentos puntuales con un objetivo claro.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Likers (fase 4), ¿cree que pueden ser una manera idónea de introducir al uso adecuado de las redes sociales y sus características? *

- (●) Sí, las actividades dan una visión bastante amplia de los detalles únicos de cada red social, aumentado la probabilidad de un buen uso futuro.
- ( ) No, es conveniente apartar estos mecanismos de contacto social alejados del menor.
- ( ) Tal vez, siempre que haya un control extremo de su uso, sin dejar margen de exploración.
- ( ) Ns / Nc.

Como docente: ¿cree que este proyecto puede ayudar a reducir el número de delitos relacionados con ciberdelincuencia? *

- (●) Sí.
- ( ) No.
- ( ) Tal vez.
- ( ) Ns / Nc.

Como docente: ¿Cree que este proyecto puede ayudar a aumentar el número de denuncias de este tipo de delitos digitales, los cuales suelen pasar desapercibidos? *

- (●) Sí.
- ( ) No.
- ( ) Tal vez.
- ( ) Ns / Nc.

Como docente: ¿Cree que este proyecto puede garantizar unas conductas y competencias en la red que mantengan a los menores protegidos dentro de sus márgenes de libertad online? *

- (●) Sí.
- ( ) No.
- ( ) Tal vez.
- ( ) Ns / Nc.

Como docente: ¿la concreción curricular es conveniente para las actividades diseñadas? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿considera los recursos de las actividades como originales y funcionales para el trabajo del alumnado? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	◉	○	Totalmente de acuerdo

Como docente: ¿Considera que la evaluación dispone de todas las herramientas y especificaciones necesarias para ser efectiva? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	◉	○	Totalmente de acuerdo

Como docente: ¿Considera que los medios dispuestos para posibles casos de diversidad funcional son suficientes? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Para finalizar puede añadir sugerencias, comentarios o mejoras al autor del proyecto: *

Trabajar a través de las emociones es fundamental. Empatizar con el alumno y ayudarlo a crecer, a aprender...

Formulario de valoración "Exploit City" (Docente)

Bienvenido/a, antes de comenzar el cuestionario le comunicaré una serie de cuestiones:

1 - Todos los datos que usted ponga en el cuestionario se usarán para fines académicos. Por tanto, solamente son un aval de que esta valoración está acreditada por los expertos o expertas correspondientes. En ningún caso se hará un uso distinto de ellos.

2 - Todas las respuestas son tomadas como valiosas, por tanto, si desea establecer ideas críticas solamente podrá beneficiar a la mejora del proyecto. Su sinceridad es primordial.

3 - Mi agradecimiento total por ayudar a completar este Trabajo de Fin de Máster con la visión experta de docentes en activo.

Dicho esto, conteste con calma las preguntas, ya que no son demasiadas. Adelante...

Nombre del docente (SOLO NOMBRE) *

Francisco

Ámbito de docencia *

Educación Primaria

Institución educativa *

CEIP San Fernando

Como docente: ¿Cree que la temática del proyecto (Introducción de conductas de ciberseguridad) es adecuada para trabajar en edades de entre 11-12 años? *

- (●) Sí, ya que en estas edades ya hay un uso importante de tecnología e internet
- ( ) No, ya que en estas edades aún no hay un uso importante de tecnología e internet
- ( ) Ns / Nc.

Como docente: ¿Considera conveniente que la escuela incluya contenidos y aspectos curriculares sobre ciberseguridad para la educación de los menores? *

- (●) Sí, considero necesario que se ahonde en el dilema con actividades y proyectos.
- ( ) No, considero que el papel de agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc.) ya es suficiente.
- ( ) No, considero que son las familias quiénes deben afrontar esta realidad por su cuenta.
- ( ) Ns / Nc.

Como docente: ¿Piensa que "Exploit City" puede ser un proyecto útil para la introducción de estos contenidos en el aula? Tenga en cuenta la respuesta que dio en la pregunta anterior. *

- (●) Sí. este es un buen ejemplo de desarrollo de conductas seguras en la red para menores.
- ( ) No, considero que este proyecto no es capaz de afrontar correctamente este dilema.
- ( ) Tal vez, siempre que hayan profesionales externos que se aseguren de la validez y solidez de la propuesta.
- ( ) Ns / Nc.

Como docente: ¿Comparte la visión de que el público adolescente puede resistirse al aprendizaje de conductas seguras en la red, siendo necesarias metodologías que "motiven" y "diviertan" a los menores? *

- (●) Sí, los niños y niñas deben sentirse cómodos al tratar estos temas que atañen a su libertad.
- ( ) No, los niños y niñas deben obtener esos aprendizajes por imposición adulta.
- ( ) Tal vez, mientras los menores no obtengan un aprendizaje equívoco de dichas conductas seguras.
- ( ) Ns / Nc.

Como docente: ¿Considera que la evasión de los derechos de autor / licencias digitales es un problema que puede corregirse en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, dotar a los menores del respeto a la propiedad intelectual evitará posibles delitos futuros en esta temática.
- ( ) No, ya que este tema es demasiado complejo como para trabajarlo en estas franjas de edad.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Commons (fase 1), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, estas actividades pueden ser un buen método de trabajo de las licencias y derechos de autoría.
- ( ) No, ya que esto puede superar lo que los pequeños y pequeñas pueden comprender.
- ( ) Tal vez, todo depende de la calidad del diseño de esas actividades y de la formación del docente.
- ( ) Ns / Nc.

Como docente: ¿Considera que el ciberacoso es un problema que debe ser abordado en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, estas edades son especialmente críticas en estos delitos virtuales.
- ( ) No, ya que estos delitos deben ser trabajados en edades de secundaria (E.S.O / Bachiller).
- ( ) Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Tegra (fase 2), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, estas actividades pueden ser una buena alternativa para conocer los peligros de cada tipo de ciberacoso y distintos sistemas de defensa ante ellos.
- ( ) No, estas actividades no ayudarán a solucionar el problema del ciberacoso o a mejorar el conocimiento sobre el mismo.
- ( ) Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ( ) Ns / Nc.

Como docente: ¿Considera que el malware o los programas malignos pueden ser abordados en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, ya que el aumento de delitos cibernéticos afecta a toda la sociedad y, por tanto, una concienciación temprana es necesaria.
- ( ) No, estos programas fraudulentos y peligros no pueden ser usados en ningún contexto en educación.
- ( ) Tal vez, siempre y cuando el contexto sea conveniente y seguro.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Black (fase 3), ¿cree que pueden ser una forma correcta de conocer el malware? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, ya que conocer bien el funcionamiento y la composición de los virus puede ayudar a evitarlos correctamente.
- ( ) No, lo conveniente es no abordar este dilema tecnológico en la escuela.
- ( ) Tal vez, siempre y cuando solamente sean métodos pasivos (antivirus, programas, etc.), dejando de lado métodos manuales para investigar.
- ( ) Ns / Nc

Como docente: ¿Considera que las redes sociales y su funcionamiento pueden ser abordados en edades escolares de Educación Primaria (11-12 años)? *

- (●) Sí, en estas edades el uso de redes sociales se dispara y no se conocen los riesgos ni condiciones de uso.
- ( ) No, las redes sociales deben evitarse lo máximo posible, eliminándolas de la realidad del menor. Por ello, no deben introducirse en ninguna clase.
- ( ) Tal vez, siempre que se usen en momentos puntuales con un objetivo claro.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Likers (fase 4), ¿cree que pueden ser una manera idónea de introducir al uso adecuado de las redes sociales y sus características? *

- (●) Sí, las actividades dan una visión bastante amplia de los detalles únicos de cada red social, aumentado la probabilidad de un buen uso futuro.
- ( ) No, es conveniente apartar estos mecanismos de contacto social alejados del menor.
- ( ) Tal vez, siempre que haya un control extremo de su uso, sin dejar margen de exploración.
- ( ) Ns / Nc.

Como docente: ¿la concreción curricular es conveniente para las actividades diseñadas? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿considera los recursos de las actividades como originales y funcionales para el trabajo del alumnado? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿Considera que la evaluación dispone de todas las herramientas y especificaciones necesarias para ser efectiva? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿Considera que los medios dispuestos para posibles casos de diversidad funcional son suficientes? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Para finalizar puede añadir sugerencias, comentarios o mejoras al autor del proyecto: *

El proyecto es muy ambicioso y tiene un detallado asombroso. Creo que sería muy procedente por parte de la Consejería analizarlo y tomarlo en cuenta para su aplicación. Muy pocos docentes son capaces de crear unos contenidos relacionados con ciberseguridad y hacerlo de manera tan eficiente. Felicidades.

Formulario de valoración "Exploit City" (Docente)

Bienvenido/a, antes de comenzar el cuestionario le comunicaré una serie de cuestiones:

1 - Todos los datos que usted ponga en el cuestionario se usarán para fines académicos. Por tanto, solamente son un aval de que esta valoración está acreditada por los expertos o expertas correspondientes. En ningún caso se hará un uso distinto de ellos.

2 - Todas las respuestas son tomadas como valiosas, por tanto, si desea establecer ideas críticas solamente podrá beneficiar a la mejora del proyecto. Su sinceridad es primordial.

3 - Mi agradecimiento total por ayudar a completar este Trabajo de Fin de Máster con la visión experta de docentes en activo.

Dicho esto, conteste con calma las preguntas, ya que no son demasiadas. Adelante...

Nombre del docente (SOLO NOMBRE) *

Alejandro Dayekh García (Autoevaluación)

Ámbito de docencia *

Educación Primaria

Institución educativa *

No procede

Como docente: ¿Cree que la temática del proyecto (Introducción de conductas de ciberseguridad) es adecuada para trabajar en edades de entre 11-12 años? *

- (●) Sí, ya que en estas edades ya hay un uso importante de tecnología e internet
- ( ) No, ya que en estas edades aún no hay un uso importante de tecnología e internet
- ( ) Ns / Nc.

Como docente: ¿Considera conveniente que la escuela incluya contenidos y aspectos curriculares sobre ciberseguridad para la educación de los menores? *

- (●) Sí, considero necesario que se ahonde en el dilema con actividades y proyectos.
- ( ) No, considero que el papel de agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc.) ya es suficiente.
- ( ) No, considero que son las familias quiénes deben afrontar esta realidad por su cuenta.
- ( ) Ns / Nc.

Como docente: ¿Piensa que "Exploit City" puede ser un proyecto útil para la introducción de estos contenidos en el aula? Tenga en cuenta la respuesta que dio en la pregunta anterior. *

- ( ) Sí. este es un buen ejemplo de desarrollo de conductas seguras en la red para menores.
- ( ) No, considero que este proyecto no es capaz de afrontar correctamente este dilema.
- (●) Tal vez, siempre que hayan profesionales externos que se aseguren de la validez y solidez de la propuesta.
- ( ) Ns / Nc.

Como docente: ¿Comparte la visión de que el público adolescente puede resistirse al aprendizaje de conductas seguras en la red, siendo necesarias metodologías que "motiven" y "diviertan" a los menores? *

- (●) Sí, los niños y niñas deben sentirse cómodos al tratar estos temas que atañen a su libertad.
- ( ) No, los niños y niñas deben obtener esos aprendizajes por imposición adulta.
- ( ) Tal vez, mientras los menores no obtengan un aprendizaje equívoco de dichas conductas seguras.
- ( ) Ns / Nc.

Como docente: ¿Considera que la evasión de los derechos de autor / licencias digitales es un problema que puede corregirse en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, dotar a los menores del respeto a la propiedad intelectual evitará posibles delitos futuros en esta temática.
- ( ) No, ya que este tema es demasiado complejo como para trabajarlo en estas franjas de edad.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Commons (fase 1), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, estas actividades pueden ser un buen método de trabajo de las licencias y derechos de autoría.
- ( ) No, ya que esto puede superar lo que los pequeños y pequeñas pueden comprender.
- ( ) Tal vez, todo depende de la calidad del diseño de esas actividades y de la formación del docente.
- ( ) Ns / Nc.

Como docente: ¿Considera que el ciberacoso es un problema que debe ser abordado en edades escolares de Educación Primaria (11 - 12 años)? *

- ○ Sí, estas edades son especialmente críticas en estos delitos virtuales.
- ○ No, ya que estos delitos deben ser trabajados en edades de secundaria (E.S.O / Bachiller).
- ◉ Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ○ Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Tegra (fase 2), ¿cree que pueden ser una solución viable para el problema? Tenga en cuenta la respuesta de la pregunta anterior. *

- ○ Sí, estas actividades pueden ser una buena alternativa para conocer los peligros de cada tipo de ciberacoso y distintos sistemas de defensa ante ellos.
- ○ No, estas actividades no ayudarán a solucionar el problema del ciberacoso o a mejorar el conocimiento sobre el mismo.
- ◉ Tal vez, siempre y cuando intervengan agentes externos (Fuerzas de Seguridad del Estado, expertos/as de la Consejería, asociaciones, etc).
- ○ Ns / Nc.

Como docente: ¿Considera que el malware o los programas malignos pueden ser abordados en edades escolares de Educación Primaria (11 - 12 años)? *

- (●) Sí, ya que el aumento de delitos cibernéticos afecta a toda la sociedad y, por tanto, una concienciación temprana es necesaria.
- ( ) No, estos programas fraudulentos y peligros no pueden ser usados en ningún contexto en educación.
- ( ) Tal vez, siempre y cuando el contexto sea conveniente y seguro.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Black (fase 3), ¿cree que pueden ser una forma correcta de conocer el malware? Tenga en cuenta la respuesta de la pregunta anterior. *

- (●) Sí, ya que conocer bien el funcionamiento y la composición de los virus puede ayudar a evitarlos correctamente.
- ( ) No, lo conveniente es no abordar este dilema tecnológico en la escuela.
- ( ) Tal vez, siempre y cuando solamente sean métodos pasivos (antivirus, programas, etc.), dejando de lado métodos manuales para investigar.
- ( ) Ns / Nc

Como docente: ¿Considera que las redes sociales y su funcionamiento pueden ser abordados en edades escolares de Educación Primaria (11-12 años)? *

- (●) Sí, en estas edades el uso de redes sociales se dispara y no se conocen los riesgos ni condiciones de uso.
- ( ) No, las redes sociales deben evitarse lo máximo posible, eliminándolas de la realidad del menor. Por ello, no deben introducirse en ninguna clase.
- ( ) Tal vez, siempre que se usen en momentos puntuales con un objetivo claro.
- ( ) Ns / Nc.

Como docente: Habiendo visto las actividades de la Corporativa Likers (fase 4), ¿cree que pueden ser una manera idónea de introducir al uso adecuado de las redes sociales y sus características? *

- (●) Sí, las actividades dan una visión bastante amplia de los detalles únicos de cada red social, aumentado la probabilidad de un buen uso futuro.
- ( ) No, es conveniente apartar estos mecanismos de contacto social alejados del menor.
- ( ) Tal vez, siempre que haya un control extremo de su uso, sin dejar margen de exploración.
- ( ) Ns / Nc.

Como docente: ¿cree que este proyecto puede ayudar a reducir el número de delitos relacionados con ciberdelincuencia? *

- ○ Sí.
- ○ No.
- ◉ Tal vez.
- ○ Ns / Nc.

Como docente: ¿Cree que este proyecto puede ayudar a aumentar el número de denuncias de este tipo de delitos digitales, los cuales suelen pasar desapercibidos? *

- ○ Sí.
- ○ No.
- ◉ Tal vez.
- ○ Ns / Nc.

Como docente: ¿Cree que este proyecto puede garantizar unas conductas y competencias en la red que mantengan a los menores protegidos dentro de sus márgenes de libertad online? *

- ◉ Sí.
- ○ No.
- ○ Tal vez.
- ○ Ns / Nc.

Como docente: ¿la concreción curricular es conveniente para las actividades diseñadas? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿considera los recursos de las actividades como originales y funcionales para el trabajo del alumnado? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿Considera que la evaluación dispone de todas las herramientas y especificaciones necesarias para ser efectiva? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	○	◉	Totalmente de acuerdo

Como docente: ¿Considera que los medios dispuestos para posibles casos de diversidad funcional son suficientes? *

	1	2	3	4	5	
Nada de acuerdo	○	○	○	◉	○	Totalmente de acuerdo

Para finalizar puede añadir sugerencias, comentarios o mejoras al autor del proyecto: *

Estos apartados lo abordaré en el propio TFE en las Conclusiones y Limitaciones u prospectiva.