Institución Universitaria

Estrategia de seguridad informática basada en gamificación, para la enseñanza en la prevención de abusos de ciber victimización por Sexting y Grooming para adolescentes de educación básica y/o media en Medellín.

Felix Alexander Usma Guzman.

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2022

Estrategia de seguridad informática basada en gamificación, para la enseñanza en la prevención de abusos de ciber victimización por Sexting y Grooming para adolescentes de educación básica y/o media en Medellín.

Felix Alexander Usma Guzman

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en seguridad informática.

Director (a):

MSc. Hector Fernando Vargas Montoya

Línea de Investigación:

Gestión de la seguridad informática

Instituto Tecnológico Metropolitano

Facultad de Ingeniería.

Medellín, Colombia

2022

Mi familia fue fundamental en todo este proceso, entender que no solo era contar con mi tiempo, mis recursos, y mis capacidades si no también con las de cada uno de ellos es reconocerles su papel en este logro, principalmente a Dios y seguidamente a ellos quiero dedicarles este trabajo y hacerles partícipes de mi alegría por este maravilloso proceso.

¿No sabéis que los que corren en el estadio, todos a la verdad corren, más uno lleva el premio? Corred de tal manera que lo obtengáis.
Y todo aquel que lucha, de todo se abstiene: y ellos, a la verdad, para recibir una corona corruptible; más nosotros, incorruptible.
Así que, yo de esta manera corro, no como á cosa incierta; de esta manera peleo, no como quien hiere el aire:

Libro de los Corintios.

Agradecimientos

Un agradecimiento especial al docente y Magister Hector Fernando Vargas Montoya, por su constante apoyo, y solidaridad al momento de trasmitir el conocimiento, y que en su tiempo fueron claves para el desarrollo de la metodología.

Agradecimiento a la Docente Maria Yolima Cárdenas, quien con su dirección fue impórtante en la creación de este proyecto, sus ideas dieron orden a la ejecución del caso de estudio y otros elementos de la ejecución.

Un fraternal agradecimiento al Profesor y Magister en educación, Juan Carlos Gutierrez Cañas quien con su conocimiento y sabiduría siempre me ayudo con la concatenación de muchas ideas en la elaboración de este proyecto.

Resumen

El uso sin supervisión de las redes sociales, las diferentes aplicaciones web que permiten una amplia interacción entre todos los individuos, la facilidad de acceder a contenidos clasificados para adultos, y el hecho de que los controles a algunas poblaciones sean menos rigurosos, han permitido que los ciber delincuentes abusen de sus víctimas con mecanismos como el sexting y el grooming afectando especialmente a la población adolescente. Una población que demanda nuevos mecanismos de aprendizaje y diferentes estrategias de prevención, que se ajusten a las nuevas tecnologías y a los diferentes entornos en los que interactúan. Poniendo esto en consideración, se propone la gamificación como una herramienta que se ajusta a diferentes estrategias y para nuestra línea de investigación orientada a la seguridad informática la usaremos como parte de la estrategia de prevención, tratando de establecer controles que además de reducir este tipo de abusos, también permitan generar conocimiento y conciencia a los usuarios de las nuevas tecnologías, relacionadas con el manejo de estas ciber amenazas. El presente trabajo ilustrará con un estudio de caso, el estado inicial y el estado final de un grupo de jóvenes estudiantes de educación media, respecto a la conciencia y conocimiento de ciber ataques como el Sexting y el Grooming, y como conclusión permitirá tener una estrategia de prevención en estos ciber ataques.

Palabras clave: Gamificación, Prevención, Abusos, Ciber victimización, Sexting, Grooming. ISO 27005.

Abstract

The use of social networks without supervision, the different web applications that allow a wide interaction between all individuals, how easy it is to access classified adult content, and the fact that the access control to some population groups is less rigorous. All of this has allowed the cyber criminals to abuse their victims, with tactics like sexting and grooming, affecting specially the adolescent population.

A population that demands new ways of learning and different prevention strategies, which fit to the new technologies and the different environments in which they interact.

Putting this into consideration, the proposal is the gamification as a tool that fits to several strategies, and for our line of research, the gamification oriented to Informatics Security, used as part of a strategy of prevention, aiming to establish security measures that also aim to reduce this kind of abuse. In addition, another objective is to generate knowledge and awareness on the users of new technologies, in regards to the correct way of dealing the cyber threats.

This research paper will illustrate with a case study, the initial and final state of a group of young students from Elementary and middle school, focusing in the awareness and knowledge of cyber-attacks like sexting and grooming. Moreover, how the conclusion will allows us to have a strategy of prevention for this kind of attacks.

Keywords: Gamification, Prevention, Abuses, Cyber victimization, Sexting, Grooming. ISO 27005.

Contenido

Lista de figuras

Pág.

Lista de tablas

Pág.

Abreviaturas

Abreviatura	Término
CAI	Comando de atención inmediato
Gaula	Grupo de acción unificada por la libertad personal
TIC	Tecnología de la información y comunicaciones
ISO	International Organization for Standardization)
ICBF	Instituto colombiano de bienestar familiar

ACIS Asociación Colombiana de Ingenieros de Sistemas

ONGs Organización no gubernamentales.

INCIBE Instituto de ciberseguridad.

Introducción

La poca capacitación tanto para maestros como para estudiantes, el desinterés por parte de las instituciones educativas y la falta de estrategias asertivas en prevención de Ciber abusos, ha causado un manejo inadecuado de los ciber ataques que están relacionados con el Ciber acoso y ciber victimización, impactando a la población de niños, niñas y jóvenes que cursan educación básica y media en la ciudad de Medellín, facilitando abusos como el Sexting y el Grooming y evidenciado en prácticas como: la Sextorsión, la afectación reputacional, Ciber bullying, entre otros, que terminan convirtiéndose en muchos casos en delitos.

Así lo demuestra la estadística tomada de la página de la policía nacional a nivel de Antioquia, durante los periodos de 2019 y 2020 en la que se evidencia la ocurrencia de 986 delitos sexuales sin empleo de armas, aunque la misma fuente indica que estos números son parciales ya que muchas personas no denuncian [1], lo que podría suponer un número más alto.

Por lo anterior, nace la pregunta ¿Cómo desarrollar una estrategia basada en gamificación para generar competencias que faciliten la identificación, prevención y manejo de ciberataques por Sexting y Grooming para adolescentes de educación media en Medellín?

La identificación de amenazas relacionadas con delitos cibernéticos, que tienen un gran impacto social, y afectan a los jóvenes con repercusiones a lo largo de su vida, como en el caso de ataques por Grooming y Sexting, nos ofrecen un campo de aplicación de los conocimientos obtenidos en la maestría para crear mecanismos en seguridad informática que faciliten la auto protección en la comunidad más vulnerable. Según los indicadores de [2] en una medida de impacto en jóvenes y niños en Colombia, se identificó que los niños de Colombia están más expuestos a riesgos cibernéticos como el acoso cibernético, los contactos peligrosos o el uso desordenado de la tecnología en comparación con los niños de otros países, en gran parte por el desconocimiento que tienen de estos delitos. Por esta razón se consideran estrategias no tradicionales de educación como la gamificación, que según diferentes fuentes [3] [4] [5] [6] ofrecen una forma muy efectiva de ayudar este grupo etario a desarrollar las competencias necesarias para identificar y protegerse.

Al analizar casos de estudio en países como España, en investigación se habla de todas las posibilidades que tienen los jóvenes y adolescentes de interactuar con las nuevas tecnologías,

desde su estudio manifiestan que el acceso a las TIC desde temprana edad promueve cambios en su vida cotidiana y la interacción con la tecnología por diferentes medios, aún desde la misma televisión, reciben una influencia dominante que desencadena en interacciones virtuales por fuera del hogar ya que los anuncios que invitan a conectarse o seguir personajes, generan motivaciones a estar conectados y desarrollar comportamientos adictivos, que finalizan debilitando la voluntad del adolescente y su resiliencia. Todos estos comportamientos y la falta de vigilancia concluyen en oportunidades para la desviación que aprovechan. En Colombia Barbosa y Ojeda [8] realizaron un análisis del comportamientos y hábitos de uso de los niños y adolescentes respecto a las nuevas tecnologías, dicho estudio revelo que los niños entre los 7 y los 10 años cuando ingresan a Internet tienen como propósito la investigación y realización de tareas, mientras los niños de 11 años en adelante buscan realizar interacciones, chats y acceso a las redes sociales, evidenciando que los cambios de conducta en los adolescentes son más agudos orientados al consumo de redes e interacciones virtuales [7].

Al revisar la estadística proporcionada por la Policía Nacional de Colombia en su CAI Virtual, y el informe de delitos del Gaula del 2020, se evidencia que los delitos sexuales a través de Internet disminuyeron. Durante el año 2020 hasta el mes de octubre en Medellín, se recibieron un total de 205 denuncias por pornografía infantil y en todo Antioquia se realizaron 986 denuncias de delitos sexuales sin empleo de armas, o de carácter virtual, en comparación al 2019, a la misma fecha en todo Antioquia se tenían 1.165 denuncias, pero que también evidencia la falta de denuncia por diferentes motivos y que en su mayoría están relacionados con miedo a la exposición o discriminación, además de la evidente pandemia que generó encierros prolongados [1].

La revolución tecnológica, los cambios en las generaciones y los abundantes recursos informáticos, han acrecentado una problemática ya existente cómo es la victimización, de esto, debemos comprender que ha ido migrando a otros planos y se ha camuflado de manera virtual, sin embargo, la ciber victimización es una problemática que ahora las organizaciones tienen que vigilar muy de cerca y que en la misma manera tienen que intensificar y actualizar los mecanismos y recursos para lograr defendernos de esta amenaza.

A mayor exposición a redes e Internet, mayor es la probabilidad que un adolescente se convierta en ciber víctima. El riesgo de ser ciber victimizado se duplica al tener un perfil en una red social electrónica, el 50% de las víctimas no comunica a nadie sobre la problemática o rara vez lo hacen,

lo que implica un riesgo mayor de volver a ser ciber-intimidado. Identificando estos factores claramente debemos hacer un análisis respecto al consumo de medios virtuales que los adolescentes de educación media están haciendo, y en medio del análisis identificar bajo qué estrategias los ciber delincuentes victimizan a los jóvenes [4].

Además, hay que considerar que con relación a la edad existe una mayor ciber victimización en los estudiantes de las edades de 14 y 18 años, frente a estudiantes de menor edad en educación media, de esta manera podemos asociar este hecho con que muchos adolescentes victimizados tengan acceso libre a redes sociales e Internet, o poca supervisión por parte de un adulto, en este sentido los ciber delincuentes encuentran más posibilidades de abusos en estas poblaciones [9]. Siempre han existido formas de intercambio de mensajes de contenido sexual [7] y siempre se ha permitido que dos individuos en el marco de sus derechos y deberes compartan entre si contenidos explícitos, sin embargo en la sociedad actual, se destaca la hiperconectividad y una velocidad de transmisión cada vez mayor, lo cual está produciendo una fenómeno donde los mensajes o información personal de carácter sexual, se reproducen con facilidad, y llegan a las manos equivocadas o en su mayoría llegan a muchos individuos sin ser el propósito principal del propietario de los contenidos reproducidos.

Luz Reyes en su ponencia de investigación documenta un relato de Sextorsión, donde una chica inicio una interacción con un desconocido, que rápidamente se ganó su confianza, al punto de pedirle que intercambiaran contenidos sexuales, entre ellos un vídeo sexual, y lo que terminó para esta chica fue una Sextorsión y que al explorar en muchos casos se identificó que este abuso se inició con una pequeña intensión de Sexting [9].

Antes que la sociedad se conectara virtualmente y evolucionara tecnológicamente, los llamados pederastas engañaban a los niños y adolescentes con elemento de encanto, dulces, globos o juguetes, para cumplir su delito y abusar del menor, sin embargo, con el cambio de los ambientes tecnológicos y las interacciones, algunos han migrado al Internet y medios tecnológicos como instrumento de avanzada, para entablar vínculos con los menores, prepararlos, engañarlos, y finalmente someterlos a abusos sexuales. A este engaño se le llama grooming, y en la actualidad es la modalidad con la cual los pederastas han alcanzado cada vez más a los menores, y les permite en ocasiones realizar muchos de estos delitos sin dejar rastro. La inmersión de niños y adolescentes en Internet gracias a las redes sociales, uso de webcams y otras tecnologías, permitió al National

Center for Missing and Exploited Children [10], estimar que una de cada cinco niñas y uno de cada 10 niños serán victimizados sexualmente de alguna forma antes de alcanzar la mayoría de edad. Al existir una mayor probabilidad de contacto entre ellos y sus agresores, al realizar un análisis de las múltiples maneras de ser victimizado un menor por un adulto, se debe evaluar también mecanismos de prevención dado que los ciber-delincuentes intensifican y diversifican la manera de victimizar, es evidente entonces, que las nuevas redes de comunicación dejan más expuestos a los menores poco educados en el manejo de las TIC y sus peligros inherentes. De allí comprendemos la constante necesidad de prevenir el abuso y conocer también el trabajo de las diferentes autoridades u organización involucradas y que tienen como fin la protección de los menores entre otros actores víctimas del abuso, conocer que el objetivo principal de los programas educativos es brindarle a los niños las herramientas necesarias para que aprendan a identificar situaciones de peligro, transgresión de límites, tocamientos inapropiados o tácticas que el abusador pueda implementar para llevar a cabo su cometido. Sin embargo, para que el propósito de prevención pueda ser asimilado por la potencial víctima es necesario diseñar mecanismos, herramientas y programas que en su orientación apunten a los individuos más expuestos; dado que al considerar también los niños más pequeños son incapaces de diferenciar el contacto sexual inapropiado [11], estos programas funcionarían modificando dicha situación.

Por otro lado, Rubio [12] en su estudio sobre el tema menciona algunos factores asociados a la ciber victimización, concluyendo que el uso frecuente de Facebook, Instagram, Twitter, Ask, acompañado de tener pocas competencias digitales los hace más vulnerables a estos Ciber acosos; teniendo presente que estas prácticas o uso de redes para las nuevas generaciones son habituales y en ocasiones no consideran los riesgos asociados. A lo anterior se le suma la poca capacitación en el tema, la falta de conciencia y el corto análisis al que están expuestos los adolescentes de educación básica y media, que genera en perspectiva, una estadística no muy favorable, que evidencia que este fenómeno se está saliendo de control y va en aumento, y por esta razón considerando el argumento de Anna Díaz [13], se deben articular todos los mecanismos y organizaciones posibles para evitar la creciente victimización por Sexting.

Así mismo, se encontró que la gamificación emerge como una herramienta de transformación educativa, de allí se comparte la idea que, si se presenta de una manera distinta el mensaje, existe la posibilidad que el receptor en este caso los estudiantes, puedan presentar mayor aceptación e interiorización de este [14]. En este sentido analizando el uso de la gamificación en la enseñanza

se identifica que el uso de este mecanismo ejerce una influencia significativa en la mejora del rendimiento de los estudiantes [15]. Así mismo se encontraron resultados significativos en la satisfacción y la actitud de los estudiantes con respecto al uso de aplicaciones gamificadas, vislumbrando un panorama positivo para la materialización de nuevas enseñanzas que están orientadas a la prevención por ciber victimización. De esta manera "*Las TIC son herramientas que van a capacitar al ser humano para que se inserte a una nueva era del conocimiento*" [16], lo cual va a exigir a la educación plantearse la creación de modelos o ambientes de trabajos encaminados al desarrollo de actitudes y aptitudes del ser humano, incluyendo la integración de los ejes transversales del plan de estudio.

Así podemos observar que la gamificación cubre de manera lúdica bien sea por medio de juegos o experiencias dinámicas, un espacio que, desde la perspectiva de algunos estudiantes, hace falta para resolver problemas de aprendizaje, además de ser una estrategia de gran importancia para el fortalecimiento de las habilidades en el reconocimiento y prevención de amenazas relacionadas con el Sexting y Grooming.

Con base en lo anterior, se tiene para este proyecto de grado los siguientes objetivos:

Objetivo general:

> Determinar una estrategia de seguridad informática, que, basada en gamificación, apoye a estudiantes de educación básica y/o media en Medellín para la identificación, prevención y manejo de ciberataques como sexting y grooming, ofreciéndoles elementos que les permiten reducir la ciber-victimización.

Objetivos específicos:

1. Establecer los diferentes riesgos que conducen al Sexting y Grooming y los impactos que son generados por estos mecanismos de ciberataques
2. Definir los controles, basados en gamificación, a los riesgos identificados, que desarrollen conciencia y toma de decisiones en los estudiantes de educación básica y/o media, respecto al uso responsable de las TIC
3. Validar elementos específicos de la estrategia que apliquen para el entorno en que se hará el estudio de caso.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

1.1.1 Gamificación

El término “gamificación” es un anglicismo ampliamente utilizado que proviene de la palabra gamification, el cual hace referencia al uso de elementos de diseño de juegos, con fines distintos a su uso normal como parte de un juego de diversión. Una manera de lograr este objetivo ha sido adaptando los métodos de enseñanza tradicionales a las nuevas teorías pedagógicas, pero también aplicando estrategias digitales haciendo uso de las nuevas tecnologías que se tienen tales como Internet, la multimedia, con mayor crecimiento en los últimos años las redes sociales y los vídeo juegos [17].

En la actualidad, la sociedad a nivel mundial se comporta como una sociedad dinámica, donde permanentemente se están dando cambios, esto supone que debemos aceptar una realidad abierta a lo desconocido. En este sentido es necesario anotar que los sistemas educativos no han evolucionado en la misma medida en que lo ha hecho la sociedad, dado que el modelo del maestro aun dicta la lección a sus estudiantes y luego evalúa bajo un examen estándar ya caducado [18]. Considerando esto y confrontándolo con la velocidad creciente de las nuevas tecnologías e interacciones a través de diferentes medios virtuales, aflora la Gamificación como un método emergente y de mucho crecimiento en los diferentes campos de la educación, mostrando un mecanismo distinto para entregar el mensaje al receptor, en este caso los estudiantes o alumnos, y que a su vez hace que sea más dinámico el proceso de aprendizaje.

1.1.2 Prevención

La prevención esta direccionada a evitar todas aquellas situaciones que desencadenen problemáticas y al mismo tiempo busca disminuir las consecuencias negativas, con lo cual, “*Prevenir, supone reducir los factores de riesgo y aumentar los factores de protección. Los objetivos principales de los programas de prevención del abuso se orientan a la evitación del abuso y a la detección temprana del abuso*” [19]

Del mismo modo Alejandra Fernández [20] expone la prevención como una estrategia pertinente y efectiva para atender a los niños, niñas y jóvenes a los cuales se les han vulnerado sus derechos o están en riesgo de ser vulnerados, es esta labor es titánica pues requiere un gran esfuerzo y una

labor cooperativa donde se involucren diferentes organismos tales como el gobierno, los profesionales y la familia. Dado que la responsabilidad es colectiva y no exclusiva de las entidades públicas con competencias en materia de protección a la infancia.

1.1.3 Abusos.

En el contexto colombiano una de las formas de victimización más comunes que se da hacia los menores de edad es el abuso sexual, dado que esta conducta es fácilmente encubierta y pocas veces denunciada por los familiares de las víctimas, esto se ha convertido en un problema intrincado y global, partiendo de factores individuales, familiares, sociales y culturales. Según manifiesta revista prisma social [21]

> *El abuso sexual es uno de los tipos de maltrato existentes y se engloba dentro del maltrato por comisión, por ser una violencia ejercida por acción buscando el daño de la víctima, por ello, este tipo es el considerado más grave para la persona que lo sufre*. [21] (p. 48)

Por tanto, es necesario generar propuestas o estrategias que trabajen hacia la prevención de ciber abusos orientados a Sexting y Grooming con herramientas de educación gamificadas o ludificadas, que permitan generar conciencia en niños, niñas y jóvenes y en sus familias. Por lo cual, es preciso tener presente [22]

> *Existan diversas definiciones de abuso sexual infantil, muchas de ellas tienen en común la presencia de tres factores. A saber, hablamos de abuso sexual, cuando se involucra a un niño en actividades sexuales de cualquier tipo, las cuales se ubican en un amplio espectro que va desde el exhibicionismo y voyerismo, hasta la penetración. Un segundo factor alude a las diferencias jerárquicas existentes entre el abusador y la víctima, indicándose que el perpetrador se encuentra en una posición de poder, al ejercer control sobre el niño. El tercer factor guarda relación con el anterior y se refiere al uso de maniobras coercitivas por parte del abusador tales como la seducción, manipulación o amenaza*. (p. 64)

1.1.4 Ciber victimización

La definición de Ciber victimización se usa para referirse al sufrimiento de agresiones de pares, por teléfono, celular o Internet, que consisten principalmente, en agresiones escritas, verbales o visuales, exclusión y suplantación [23]

Los estudiantes se enfrentan no solo a la victimización tradicional, sino también a la ciber victimización. A medida que los teléfonos celulares, los teléfonos inteligentes y las computadoras

personales se vuelvan más accesibles y confiables para la comunicación, es probable que la victimización cibernética sea más común. [24]

1.1.5 Sexting - Un intercambio sin control.

El término "Sexting" es un vocablo incorporado de manera completo en la literatura hispanoparlante que significa envío y recepción de mensajería con imágenes o fotografías que presentan un contenido sexual especifico, a través de Internet o dispositivos como celulares o tabletas. Muchas, por no decir la mayoría o la totalidad de estas imágenes, se distribuyen de manera inmediata, sin control y masivamente a través de las redes sociales.

El Sexteo término que implica la distribución de imágenes o vídeos con contenido sexual a través de las redes sociales ya sea con o sin autorización de los propietarios. La divulgación de estos contenidos es instantánea, con consecuencias prácticamente siempre graves para los niños, niñas y jóvenes. [3]

También se puede afirmar que “la violencia online adquiere especificaciones como: Sexting, el cual consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de celulares” [9]

Fig. 2-1. Ciclo de Sexting hasta llegar a la sextorsión. [1]

En la fig. 2-1 se brinda una descripción de como progresivamente se es víctima, partiendo desde un tierno alago o conversación, hasta llegar a la intimidación o sextorsión y finalmente la publicación de contenidos sexuales personales en internet.

1.1.6 Grooming – El engaño que evolucionó.

Es un conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través de Internet, con el fin último de obtener concesiones de índole sexual [9]
El texto predadores sexuales online y menores: [25] “Se incrimina como la conducta consistente en contactar un menor de edad por medios tecnológicos, proponiéndole concertar un encuentro, acompañando dicha propuesta con actos materiales encaminados al acercamiento y con la finalidad de cometer delitos contra la integridad sexual”. (p. 2)
A demás de las anteriores definiciones, se toma como estadística la base de datos de medicina legal en Colombia, y específicamente en el departamento de Antioquia informo que se presentaron durante el año 2020, 726 delitos sexuales sin empleo de armas entre los cuales está el ciber delito o abusos [1]

1.1.7 ISO 27005

La Norma ISO 27005 del 2018 Es un estándar internacional encargado de la gestión de riesgos de seguridad de la información. Dicha norma contiene las directrices que se deben realizar para llevar a cabo el proceso de gestión del riesgo, y es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que amenacen la seguridad de la información de su organización. [26]

Finalmente, se precisa que este es el soporte conceptual de todo el proyecto de grado, no es un glosario, es una identificación y claridad de los diferentes componentes usados en el desarrollo del proyecto y que permiten dar a conocer (explicar) su uso posterior.

1.2 Estado del arte

Partiendo de la línea seleccionada para trabajar en el proyecto de investigación, se realiza una revisión bibliográfica sobre el tema estrategia de seguridad informática basada en gamificación, para la enseñanza en la prevención de abusos de Ciber victimización por Sexting y Grooming para adolescentes de educación básica y media. Inicialmente, en bases de datos bibliográficas como Dialnet, Scielo, Springer link, Redicuc, Mendeley y otras fueron consultadas, además se consultó también en bases de datos de la Policía Nacional de Colombia y medicina legal.

El texto, Pensamiento computacional en las escuelas de Colombia, colaboración internacional de innovación en la educación, propone profundizar las evidencias modernas, sobre la huella que deja el trabajo con aplicaciones gamificadas en el progreso y aumento del rendimiento de los estudiantes en la enseñanza de la Informática. Las conclusiones obtenidas permiten ver que el uso de la gamificación produce un efecto significativo en la mejora del rendimiento de los estudiantes [17].

Esta investigación siguió un enfoque metódico con parámetros acordes a las instituciones educativas, los profesores y los alumnos, y como resultado en la mayor parte de los alumnos, se pudo evidencias que el uso de la aplicación gamificada (7 de 10), ayudo a promover en los estudiantes un cambio en su comportamiento, y como resultado un avance en su rendimiento académico, además se encontró que los procesos que se han empleado para evaluar la mejora en el rendimiento de los estudiantes al usar aplicaciones gamificadas, se determinaron principalmente de manera cuantitativa. Además de evaluar la mejora en el rendimiento, se han evaluado también la satisfacción y la disposición de los alumnos respecto al uso de las aplicaciones gamificadas.

Montiel y Agustina firman que las Redes Sociales les facilitan a los jóvenes a mantenerse en contacto e interactuar con otros, (es decir, amigos y familiares u otras personas con intereses similares), pero también los entretienen y les brindan una nueva forma de aprender. Sin embargo, dado que los adolescentes se benefician del uso de las redes sociales, también están expuestos a los riesgos al interactuar, publicar o compartir información en las redes sociales. Por tanto, necesitan una formación adecuada para potenciar su desempeño actual y futuro en las redes sociales. Los centros educativos y las administraciones públicas han llevado a cabo diversas estrategias educativas para potenciar la conciencia de los usuarios adolescentes sobre los riesgos de privacidad, y reducir su exposición al Ciber acoso derivado del uso de las Redes Sociales, (como nuevos consumidores y usuarios), evitando posibles consecuencias negativas o experiencias que los incomoden en las Redes Sociales [7].

Estudios previos que han evaluado el impacto de las iniciativas educativas, sugieren que estas estrategias tienen éxito en aumentar la conciencia sobre los riesgos en línea. Sin embargo, la comunidad investigadora considera que la conciencia no necesariamente impulsa conductas poco riesgosas entre los niños, niñas y jóvenes. Este efecto concuerda con la cantidad de jóvenes que informan vivencias negativas en la red pese a los diferentes proyectos y campañas ejecutadas por

las instituciones educativas. Como opción a los materiales pedagógicos, se ha propuesto el uso de herramientas tecnológicas como un medio de ofrecer experiencia práctica para aprender actitudes y comportamientos adecuados al utilizar sitios de redes sociales. La inclusión de la gamificación es de interés para el diseño de actividades que estén orientadas a obtener una retroalimentación positiva, la gamificación social tiene como objetivo unir la gamificación y las redes sociales para combinar el potencial de los dos enfoques, con el fin de crear experiencias de usuario atractivas impulsadas por las redes sociales. Desde una perspectiva educativa, las redes sociales facilitan la comunicación y las interacciones entre los estudiantes y con los profesores y resaltan los elementos de contenido relevantes. Su potencial también se puede aprovechar para cooperar y crear conversaciones significativas en las interacciones de aprendizaje. Por otro lado, la gamificación estimula aspectos motivacionales, como la participación y el compromiso con los contenidos de aprendizaje y con otros participantes, además, se pueden mejorar diferentes habilidades como la competitividad, la colaboración y la adaptación en función de los instrumentos de gamificación utilizados. La integración de instrumentos de gamificación en contextos ajenos al juego para enseñar a las personas de manera práctica sobre tareas aburridas, tediosas o complejas está ganando popularidad. El concepto de privacidad, y especialmente la privacidad de los usuarios en las redes sociales, es un desafío que se destaca en varios trabajos de investigación. Por lo tanto, el uso de la gamificación en el contexto de las redes sociales para enseñar a los usuarios sobre la privacidad y los mecanismos de privacidad de la red social es una combinación perfecta. Esta combinación permite a los usuarios ser conscientes de su privacidad y así poder gestionar mejores escenarios complejos para evitar posibles fugas de información o arrepentimientos [7].

Videojuegos y tic como estrategias pedagógicas [27], permitió conocer antecedentes específicos respecto al uso de videojuegos para la enseñanza y otros procesos educativos respecto a incidentes asociados al uso de Internet (Ciber acoso, Sexting, Grooming, pornografía infantil, etc.), establece los videojuegos como estrategias importantes a nivel pedagógico por las posibilidades que ofrecen de ser usados en calidad de narrativa digital, herramienta o entorno de aprendizaje, cuya implementación trasciende del ámbito comercial al pedagógico. Proponiendo que el tema de redes seguras se ha constituido en una de las principales preocupaciones de los diferentes entes en el ámbito nacional e internacional, principalmente por las problemáticas derivadas del uso de Internet, redes sociales, y la falta de regulación, por esto se reflexionó, realizar un rastreo respecto el uso de videojuegos en ambientes pedagógicos, de esta manera como echar de ver experiencias

de proyectos para el establecimiento de medios TIC, como herramientas didácticas para la formación, sea el asunto especifico del empleo de videojuegos y otros materiales interactivos, se centró principalmente en la investigación de datos y estudio del material encontrado, en los temas de Internet Seguro, como “Gamificación y educación”, “Presentación de avances del proyecto Internet seguro”, “Elaboración de guiones para videojuegos”, “Proyecto y conjunto de exploración Nipón Estudio Anime”, “Nuevas Dinámicas en Grupos de Investigación”, dirigido a estudiantes de formación básica secundaria y superior, posteriormente de las indagaciones encontradas se presentan los aportes de experiencias partiendo de aquellas que trabajan sobre la problemática, continuando con las que utilizan el mismo método o similares y finalizando con problemáticas o subtemas centrales como el Grooming, los Ciber - (bullying -dependencia, -pornografía, -sexo), los sex- (Sexting, Sextorsión), y la pornografía infantil.

En la investigación nuevas tecnologías y victimización sexual de menores exponen que las teorías e investigaciones criminológicas vienen tratando de identificar los factores de riesgo y de protección, con la finalidad de comprender con mayor profundidad los procesos de victimización y mejorar las estrategias de prevención. En este contexto, conviene avanzar en programas educativos que tengan en cuenta las carencias y vulnerabilidades mediante el análisis de las concretas formas de Ciber victimización, se pretende señalar algunas pautas basadas en la investigación criminológica, partiendo sin duda, que el ser humano en la era digital presenta junto a otras consecuencias positivas, una mayor vulnerabilidad. Más allá del transhumanismo, conviene poner el foco de atención en los cambios antropológicos que, en sí mismos, producen los cambios tecnológicos en la esfera del obrar humano en todas sus dimensiones: percepción, conocimiento, aprendizaje, comunicación, interacción y, eventualmente, victimización. La anticipación en la edad de acceso a las TIC experimentada en los últimos años, ha supuesto cambios muy significativos en las actividades cotidianas en el ciberespacio por parte de los menores y como resultado para prevenir la Ciber victimización infanto-juvenil no basta con educar en competencias tecnológicas, la verdadera preparación para un buen uso de las tecnologías reside en la comprensión del contexto [5].

Villacampa en dos estudios busca conocer la realidad tanto del padecimiento de Grooming, como de la intervención en Sexting de los adolescentes en España. Para esto, se llevó a cabo una investigación cuantitativa con una muestra de 489 estudiantes de secundaria en Cataluña, los cuales se encuentran entre los 14 y los 18 años, y concluye que la cruzada originariamente

emprendida en Estados Unidos contra los predadores sexuales adultos con la generalización de las tecnologías de la información se ha dirigido después contra los propios adolescentes y se sancionan por conductas relacionadas con el Sexting consensual entre iguales. Además, entre los hallazgos se encontró que para el caso del Grooming el nivel socioeducativo de los padres sí se observó que tenía significación para explicar esta victimización [5, 25].

La revista Espacios en su artículo Prácticas de riesgo en Redes Sociales y WhatsApp por estudiantes de educación básica secundaria analiza los riesgos asociados al uso de Internet en niños y adolescentes desde una perspectiva transcultural. Con la colaboración de alumnos de básica secundaria de la provincia de León – España y del departamento de La Guajira – Colombia, en el cual los alumnos de formación secundaria se hallan en proceso de experimento de diversos cambios producto de la juventud, un período progresivo de la persona donde se exhibe problemas de autorregulación, se aprecia la necesidad de aprobación, y de conservar una imagen ante el grupo, lo que conlleva en querer estar hiperconectados a la red [28].

Asimismo, nace interés por relacionarse con desconocidos, por examinar la sexualidad, y por conocer contenidos impropios. De esta manera brotan peligros que pueden ser pasivos o activos en la medida en que se accede tanto de manera premeditada como impensada a contenidos no adecuados para la edad, se admiten invitaciones de desconocidos, y se desenvuelven conductas delictivas con el uso de Internet. El diseño metodológico usado es instrumental transeccional, no experimental de corte comparativo. En tal sentido es instrumental transeccional porque se establece la medición con el uso de la Escala de factores de riesgo asociados al uso de las Tecnologías de Información y Comunicación (TIC) y se estableció la posibilidad de comparar dos muestras de estudiantes del nivel básico secundario, residentes en dos contextos culturales diferentes (Provincia de León – España, y el departamento de La Guajira – Colombia). Constatan con base en el estudio que no existen diferencias significativas entre las dos regiones frente a los patrones de uso de Internet los que nos permite inferir que siendo dos regiones tan apartadas geográficamente estos patrones deben ser similares para el grupo etario en general.

En algunos trabajos relacionados (tabla 2-1) se encuentra una gran contribución de la gamificación en temas de prevención e investigación, que permiten fortalecer esta propuesta de profundización.

Tabla 2-1
Contribuciones de la gamificación.

Trabajo Relacionado	Contribución	Propuesta.
Concepciones éticas sobre el uso de las tic de los estudiantes de la institución educativa Octavio Harry de Medellín, grados 8° a 11°, desde el pensamiento crítico, la autonomía y la responsabilidad [43]	La comprensión de un fenómeno contemporáneo, como es el uso honesto y responsable de las TIC, desde las concepciones ética en el uso de estas por parte de un grupo de estudiantes de los grados octavo a undécimo de una Institución Educativa Oficial del Municipio de Medellín,	Proponer de acuerdo con los hallazgos de la investigación, estrategias pedagógicas, que puedan ser incluidas en los planes del área de Ética y tecnología, para fortalecer la formación de los estudiantes, como aporte a la promoción, prevención, uso honesto y responsable de las TIC
Modalidades delictivas que se desarrollan a través del Sexting en Colombia: un análisis comparado con España y estados unidos [44]	Identificar el concepto y evolución del `Sexting´ y las conductas punibles que puede derivar su utilización, además realizar un análisis comparado a través de la revisión de pronunciamientos judiciales sobre el `Sexting´ como figura delictiva o generadora de otras conductas punibles entre Colombia, España y Estados Unidos.	La presente investigación, se ocupará exclusivamente de las conductas punibles que acarrean la divulgación de imágenes o videos íntimos, práctica denominada `Sexting` y otras modalidades que se derivan de esta, y con las que se puede incurrir en la comisión de varios tipos delictivos. Un análisis comparado permitirá reconocer la gravedad de estas conductas en Colombia, España y Estados Unidos.
Diagnóstico de riesgos asociados al uso de internet en niños: un camino para la prevención a través de narrativas transmedia [45]	Proponer un prototipo funcional bajo los lineamientos del diseño de contenidos transmedia para la prevención de los riesgos del uso de internet para la población objetivo en la ciudad de Medellín	Diseñar una propuesta de prevención de los riesgos asociados al uso de internet para medios digitales en clave del diagnóstico de la población objetivo.

Acorde a lo anterior, diferentes autores han investigado sobre el tema de gamificación o sobre el ciber acosos, pero no se evidenció la forma cómo estos dos elementos pueden unirse para dar una solución clara a la problemática en el uso de las TIC.

2. Metodología y Resultados.

En este capítulo se define la metodología y los resultados de manera inmediata. A nivel teórico, se profundizó un tema que en el Municipio de Medellín tiene pocas referencias, ya que al rastrear en las bases de datos científicas, policiales y relacionadas con educación se encuentra poca información respecto a usar la gamificación como mecanismo de prevención en Ciber abusos, que además plantee una estrategia en el trabajo contra Ciber crímenes orientada hacia Grooming y Sexting. Por tal motivo, se desarrolló una estrategia de seguridad informática basada en gamificación donde se probó mediante un estudio de caso, una de sus guías, para validar de forma

experimental el impacto y los resultados. El trabajo se desarrolló con el cumplimiento de los diferentes objetivos específicos, considerando fases para cada uno de en la gráfica 2-2.

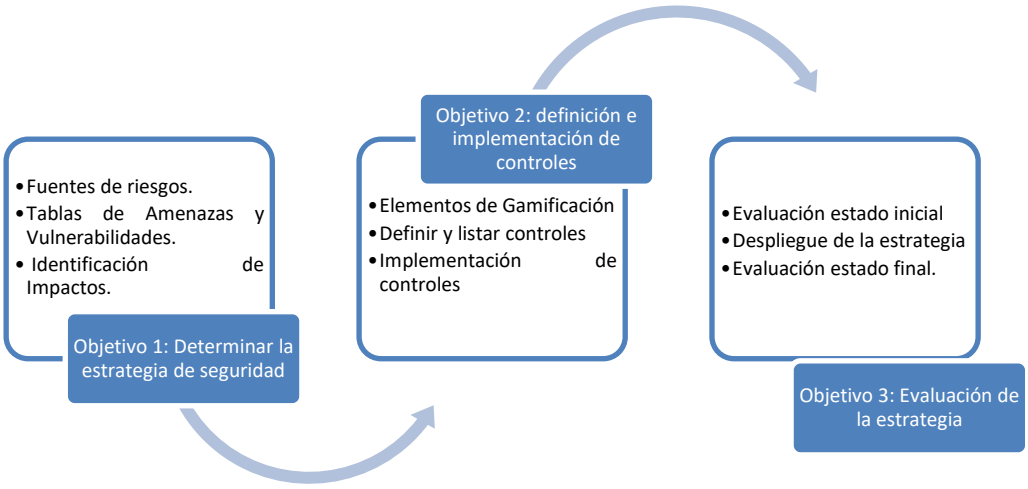

Fig. 2-2: Consolidación de fases para el desarrollo de cada objetivo. Fuente propia Fuente propia

En el cumplimiento de los objetivos uno y dos se tomó como marco referente la norma ISO 27005 de 2’018 en algunos de sus contenidos, de esta manera poder tener un punto de referencia al momento de analizar situaciones mencionadas en sus respectivas fases como lo son, evaluación del riesgo, el tratamiento de los riesgos, la aceptación del riesgo, implementación de controles, entre otros.

En el establecimiento del contexto se realizó una identificación de la población y las causas que conllevan a los riesgos Sexting y Grooming.

En la identificación de los riesgos, se establecieron aspectos como lo son amenazas, vulnerabilidades, riesgo e impacto.

En el proceso de tratamiento de riesgos fue fundamental la identificación de amenazas y vulnerabilidades de esta manera se establecieron los diferentes controles a los riesgos ya identificados.

A continuación, se da la descripción de la metodología usada para cada objetivo, así como los resultados en el mismo capítulo.

2.1 Objetivo específico 1: Establecer los diferentes riesgos que conducen al Sexting y Grooming y los impactos que son generados por estos mecanismos de ciberataques.

2.1.1 Identificación de fuentes de riesgos.

Para el desarrollo de esta actividad, se tuvo en cuenta fuentes como ICBF, DQinstitue, Universidad EAFIT, TIGO-UNE, ACIS, entre otras, en las cuales se realizó búsquedas relacionadas con el uso y consumo de internet por parte de los niños y jóvenes, analizando que tipo de comportamientos podían derivar de los excesos en estos usos, las características de la información que se analizó eran mayormente datos estadísticos y con proceder en riesgos como el Sexting y el Grooming, usando esta información para la justificación de la fase.

Para el desarrollo de esta actividad se tuvieron en cuenta las siguientes fuentes:

- https://www.dqinstitute.org/impact-measure/#impactresearch
- https://contigoconectados.com/resultados/uso-y-acceso/
- Https://www.icbf.gov.co/
- https://www.acis.org.co/

Resultados fase 1:

Acorde a lo definido en la metodología, se procedió a realizar las diferentes consultas, con el fin de encontrar y tabular la información relevante asociada los posibles riesgos asociados al Sexting y Grooming.

El origen de los riesgos asociados a la ciber victimización por Sexting y Grooming puede tener variaciones dependiendo del contexto en el cual se evalúe y los diferentes elementos que involucren al individuo, como lo detallan diferentes organizaciones que protegen la infancia y la adolescencia, además que evalúan temas relacionados con el riesgo en estas poblaciones.

Al realizar el análisis de comportamiento y riesgos de los niños en Colombia respecto a los niños de otros 29 países (Fig. 2-3), se logró identificar que Colombia obtuvo una puntuación alta en relación con los riesgos cibernéticos ocupando la posición 26°, los contenidos de riesgo ocupando la posición 27° y los contactos de riesgo posición 26° [2].

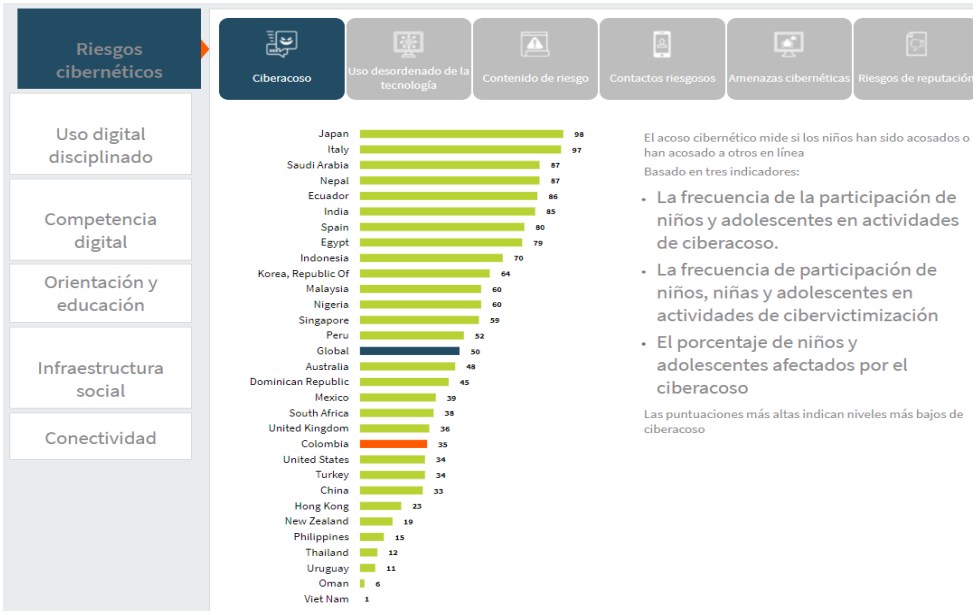

Fig. 2-3. Informe Nivel de riesgos. [2]

Sin embargo, el no tener un rango alto de riesgos cibernéticos en comparación con los otros países del estudio que realiza DQINSTITUT (fig. 2-3) si se han identificado factores de riesgo que requieren atención especial, y que, para investigación del origen de riesgo propuesta para este trabajo, se identifican porcentajes de afectación que requieren vigilancia especial.

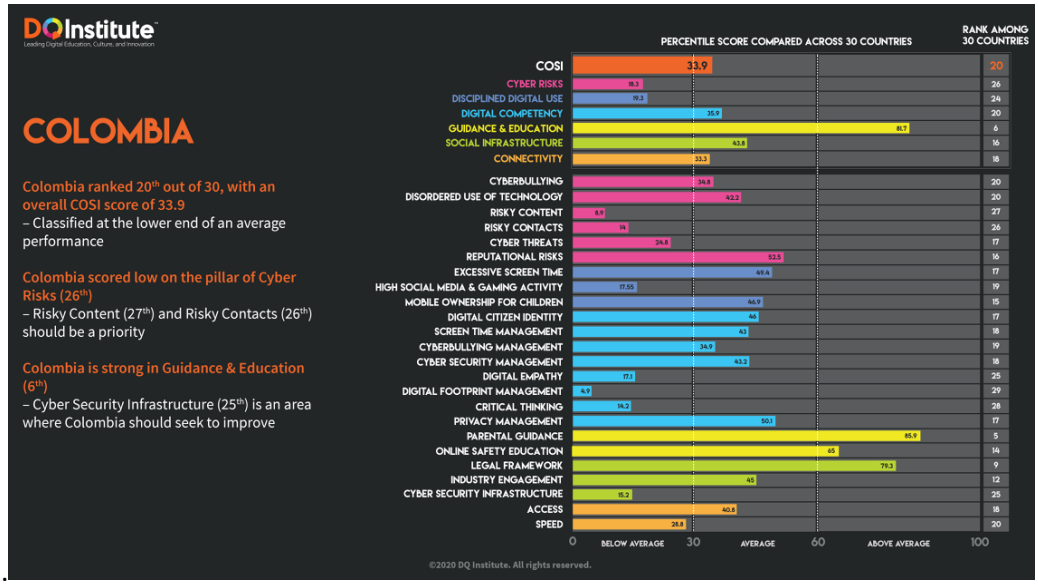

Fig. 2-4. índice de seguridad infantil en línea. [2]

Algunos factores u orígenes de riesgo están coligados a componentes poco reforzados o incluso no trabajados en nuestro país (gráfica 2-4), como es el caso del indicador de gestión de huella digital con un porcentaje de 4.9%, que evidencia una contundente falta de disciplina digital que es otro indicador que quedó muy bajo con un porcentaje de 19.3%, y que en efecto no es algo bueno ya que nos deja entre ver que los niños y jóvenes no tienen en consideración un buen tratamiento de su información o sombra digital, estos dos indicadores son la evidencia de la mala administración de su identidad en internet[2].

También se encontró algunos comportamientos específicos que se determinan como fuentes de riesgo y que están asociados al uso de las tecnologías de la información, tales como la elevada frecuencia de uso de las tecnologías de la información y la comunicación (la mayor experiencia tecnológica o el uso de estas tecnologías por períodos prolongados) el tiempo de conexión a Internet: a mayor tiempo de conexión a Internet mayor riesgo de convertirse en víctimas de Ciber acoso [29].

De acuerdo con ACIS (asociación colombiana de ingeniería) la cual determinó que el 15% de los niños en Latino América pasa más de cuatro horas conectado a internet mediante un dispositivo móvil, y quienes llevan la delantera al respecto son los menores argentinos con 24%, seguidos por chilenos (21%) y brasileños (18%). Más atrás se ubican colombianos (12%), peruanos (7%) y mexicanos (7%) [30].

De acuerdo con la investigación realizada por la universidad EAFIT y Tigo-Une, los niños y adolescentes del país gastan aproximadamente tres horas y media diarias para navegar por internet. La mayoría de las veces esto se hace mediante un dispositivo inteligente como celulares, tablets y computadores de uso propio. El estudio tuvo en cuenta 485 encuestas a niños y jóvenes entre 9 y 16 años [31].

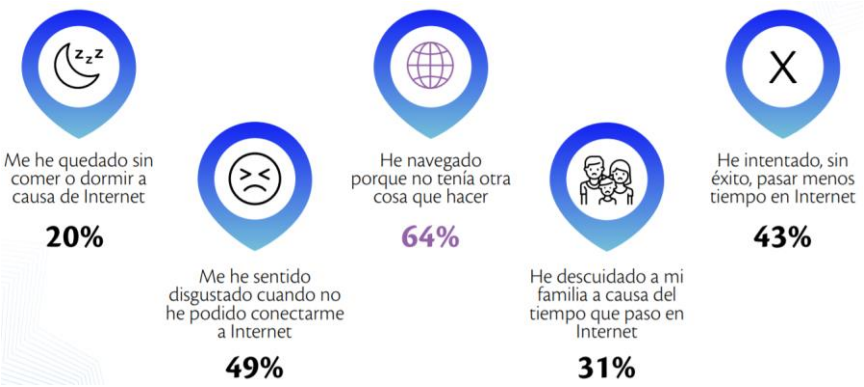

Fig. 2-5. Consumo de internet y redes. [31]

Como se muestra en la fig. 2-5 del estudio de la universidad Eafit y Tigo-Une, el 20% de los menores de edad de entre 9 y 16 años deja de dormir por usar redes sociales, algunos estudios señalan que el riesgo de ser ciber-víctima se duplicaba al tener un perfil en una red social.

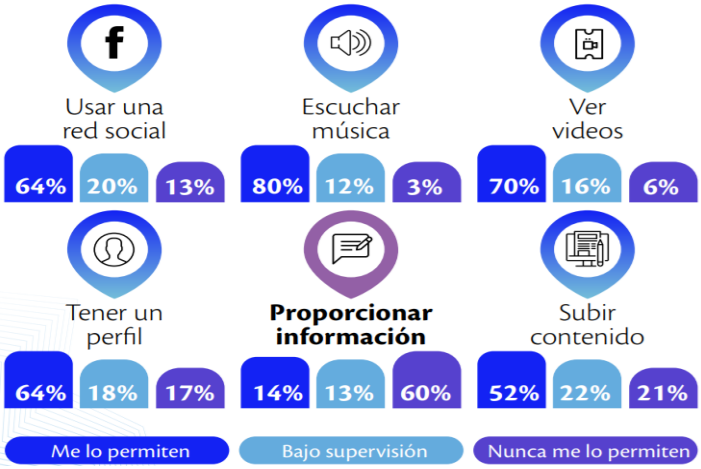

Fig. 2-6. Acciones en internet y redes. [31]

En ese orden ACIS (asociación colombiana de ingeniería), afirma que El 45% de los niños en Colombia tienen perfil y el 15% de los padres desconoce lo que publican.

A partir de la información que se visualiza en la fig. 2-6, identificamos que casi la mitad de los niños en Colombia entre los 9 y los 16 años tienen redes sociales y además de esto, que en un alto porcentaje muchos no tienen una supervisión al momento visitar estas redes sociales, por lo tanto, este número que no tiene supervisión o acompañamiento se convierten en potenciales víctimas de ciber delitos como lo son el Sexting y el Grooming [30].

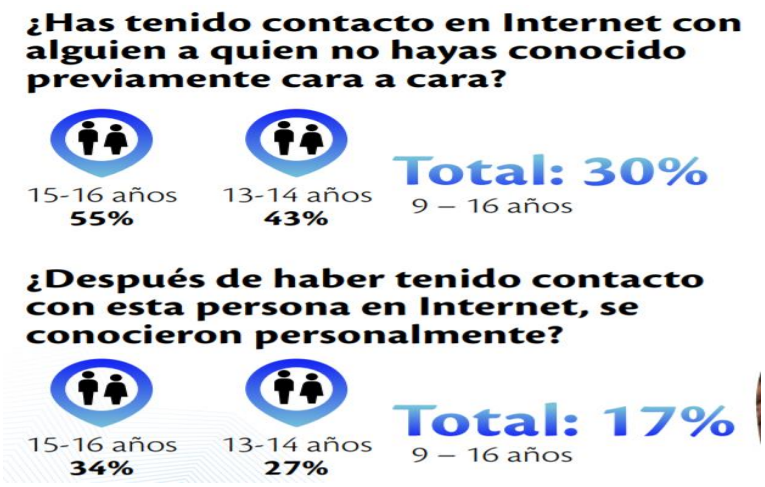

Fig. 2-7. Contacto con desconocidos. [31]

Hacer uso de los servicios de mensajería instantánea, cámaras web y chat facilita el contacto con desconocidos fig. 2-7, lo que incrementa el riesgo de ser intimidados en línea.

Datos obtenidos de ICBF indican que en Colombia el 30 % de los menores de edad encuestados ha conocido gente por internet y, de este grupo, el 17 % manifestó haber tenido encuentro cara a cara con sus nuevos amigos virtuales. Lo que potencialmente incrementa la posibilidad de ser víctimas [31].

Por otro lado, el 84% de los niños y jóvenes colombianos de entre 9 y 16 años ya tienen perfiles en las principales redes sociales, a pesar de que estos sitios solo permiten su apertura a partir de los 13 años.

Con respecto a la visualización de contenidos sexuales, el 24% dice haber accedido a ellos a través de las redes sociales; 13% son sorprendidos por una ventana emergente, y otro 10% los encuentra en videos y películas, finalmente se indica que un 7% reconoce haberlos visto en páginas para adultos y otro 3% en juegos en línea, en la Fig. 2-8 observamos que el riesgo es tanto como para niños y niñas estando dividida la estadística encuestados en porcentajes iguales. [31].

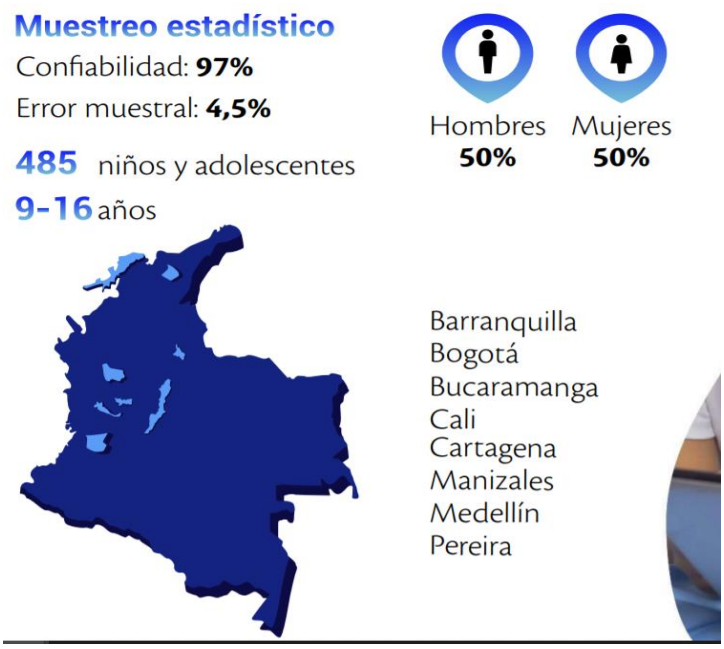

Fig. 2-8. Niños de 9-16 años que visualizaron pornografía. [31]

Así lo indica la academia estadounidense de pediatría donde informa que los niños y los adolescentes de hoy están creciendo inmersos en los medios digitales y están expuestos a estos en diferentes formas, tales como la televisión, los computadores, los teléfonos inteligentes y otras pantallas, los medios de comunicación pueden influenciar a los niños y a los adolescentes e impactar su bienestar, la forma en que aprenden, piensan y se comportan [29].

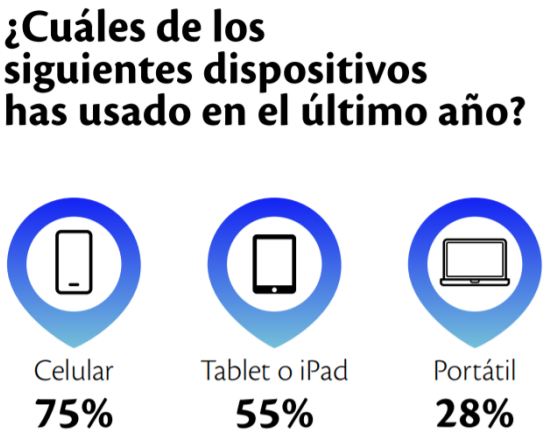

Fig. 2-9. Dispositivos más usados por los Niños de 9-16 años. [31]

Como muestra la fig. 2-9 el 75 % de los adolescentes tienen acceso a un teléfono inteligente, de esta manera se entiende que también tienen acceso al internet, ven televisión, videos y descargan

aplicaciones (apps) interactivas, estas aplicaciones para móviles permiten compartir fotos, jugar y hablar por video chats, también se encontró que 4 de cada 5 hogares (familias) poseen un dispositivo para jugar videojuegos.

Falta de compromiso, desconocimiento por parte de los padres o cuidadores respecto al uso de las redes e internet.

Esta falta de compromisos o desconocimiento, en la mayoría de los casos se convierte en poca supervisión y mala gestión de las actividades y acciones de los niños y adolescentes en el uso de las redes e internet.

Al realizar un análisis de consumo de redes sociales es proporcional a los jóvenes y adolescentes que tienen perfil o cuenta en una red social, y de la misma manera también se evidencia que los encuestados que tienen cuentas y usan estas redes, también comparten contenidos y suben o publican información [31].

Estos son algunos de los factores que se asocian con la victimización cibernética, que al explotarse pueden derivar en Sexting y Grooming.

2.1.1.1 Tablas de amenazas y vulnerabilidades.

Tomando como referencia los anteriores factores de riesgo que se identificaron, se realizó una tabla de amenazas y vulnerabilidades consolidada (tabla 2-2), que explotadas podrían terminar en ciber victimización por ***Grooming*** (generando un alto impacto en las personas).

Tabla 2-2.

Establecimiento de riesgos, amenazas y vulnerabilidad por Grooming Elaboración propia.

Riesgos	Amenazas	Vulnerabilidades
GROOMING	Abuso infantil.	Prolongados y extensos tiempos navegando en las redes sociales e internet.
		Aceptar solicitudes de desconocidos.
		Compartir información personal y de ubicación en redes e internet.
		Ceder a chantajes y extorciones.
	Ciberacoso.	Establecer relaciones estrechas con personas de rango de edades distantes.
		No denunciar acercamiento de terceros, con proposiciones delictivas.
		Poca supervisión de un adulto o cuidador.
	Sexting.	Recibir incentivos por acceder a solicitudes de algún tercero.
		Intercambiar contenidos sexuales.
		Enviar y recibir fotos e información personal.

la tabla 2.2 nos permite evidenciar las vulnerabilidades, amenazas que culminan en la explotación del grooming como riesgo, estos datos acordes a la información de las fuentes de riesgos presentadas en el punto 2.1.1 del presente trabajo.

Tabla 2-3.

Establecimiento de Riesgos, amenazas y vulnerabilidad Por Sexting. Elaboración propia

Riesgos	Amenaza	Vulnerabilidad
SEXTING	Robo de información, contenidos y fotos	Cuentas en redes sin control de seguridad
		Contraseñas poco seguras o genéricas
		Usar redes públicas, de parques, CC comerciales o colegios.
		Compartir contenidos personales y explícitos en redes sociales públicas.
		Fata de capacitación en el manejo de redes e internet.
	Distribución o publicación de fotos privadas o de contenido explicito.	guardar fotos, medios o contenidos explícitos y privados en cualquier repositorio
		compartir fotos del cuerpo con poca ropa.
		Establecer relaciones vía web en las cuales se considere la trasferencia de contenidos sexuales.
	Sextorsión.	Participar de la práctica de sexting.
		Acceder a pretensiones de desconocidos.
		No denunciar ante autoridades correspondientes.
		Establecer relaciones virtuales con desconocidos.
	Ataques físicos.	Confiar plenamente en la discreción del destinatario
		Sentir presión de grupo que lleve a ganar notoriedad y aceptación en el contexto digital
		Temor a perdida reputacional.

Acorde a las tablas anteriores (tabla 2-2 y tabla 2-3), se puede apreciar que para el Grooming se identificaron 3 amenazas y 10 vulnerabilidades, en el caso del Sexting se identificaron 4 amenazas principales y 15 vulnerabilidades, lo que supone un alto riesgos para los niños y jóvenes que están en contacto permanente con la tecnología o que tienen acceso a todos los recursos digitales sin una debida capacitación o acompañamiento.

2.1.2 Identificar el impacto del Grooming y Sexting.

En el desarrollo de esta actividad o fase se realizaron consultas en diferentes fuentes y bases de datos institucionales, académicas y abiertas como ICBF, CAI Virtual, Europol, entre otras, buscando información relacionada a los impactos que pueda generar el explotar vulnerabilidades asociadas el sexting y grooming, además de una descripción de algunos de esos impactos.

Desafortunadamente el haber sido víctima por Sexting y Grooming no permite enumerar impactos positivos o listar buenas conclusiones más allá de las lecciones aprendidas, los impactos que pueden generar estas vulnerabilidades podrían variar en solo un pequeño susto, hasta aspectos legales con efectos físicos y emocionales.

Algunos de los impactos más relevantes son:

Perdida reputacional: Si las fotos privadas se ven comprometidas, podrían acabar publicadas en páginas web de pornografía. Esto podría dañar la imagen de la víctima tanto en la red como en la vida real y crearle graves problemas. Además, los familiares o compañeros de trabajo de la víctima podrían ver estas fotos y esto podría causar un gran impacto en su vida [9, 32].

Sextorsión: La extorción como mecanismo de delincuencia se trasforma cada día, aplicando nuevas técnicas y ataques a sus víctimas, además de aprovechar la falta de cautela de los usuarios de dispositivos electrónicos como celulares, Tablet y computadores, ahora ha pasado a capturar información íntima o personal de cuentas en diferentes portales, en la nube o alojada en diferentes recursos, esta información la usan como gancho o bandera para tomar lo que quieren de las víctimas, en el caos de contenidos sexuales o explícitos, intimidan a los propietarios de esta información para que acceda a peticiones con el propósito de no exponer la información, muchas de estas intimidaciones terminan siendo aceptadas por la víctima que finalmente paga un precio económico y en muchas ocasiones terminan realizando acciones en contra de su voluntad o integridad [32, 33].

Prostitución: De acuerdo con el portal de la policía nacional de Colombia, existen evidencias donde se encontraron casos de mujeres y hombres que, por delitos de Sextorsión asociados al Sexting, que terminaron en actividades como prostitución o webcam, aunque no se tenga una estadística clara de esta problemática, es un riesgo que se puede presentar [34, 37].

Problemas psicológicos: Sucede cuando relaciones sentimentales que fueron muy afectivas compartían imágenes muy eróticas, terminan en decepciones amorosas hasta llegar a la ruptura, y con consecuentes de tal medida que algunas de estas personas que conservan dichos contenidos de las relaciones deciden vengarse y una de las formas más sencillas es compartiendo dicho material íntimo, la persona expuesta y afectada sufre una daño moral y sociológico ya que esto le desestabiliza mentalmente y además que no se sabe cómo actuar o a quien acudir por temor a represalias o más exposición [35].

Problemas económicos: Una persona sometida a chantajes e intimidaciones derivadas del Sexting puede, en algún momento, presentar problemas económicos si no denuncia oportunamente o si accede a las peticiones del victimario [33].

Abuso sexual: Un niño o adolescente que fue victimizado por un ciber delincuente puede terminar siendo perpetrado sexualmente, lo que se convertiría en un abuso sexual, uno de los impactos más terribles del Grooming [7, 10, 36].

2.2 Objetivo Especifico 2: Definir los controles basados en gamificación a los riesgos identificados, que desarrollen conciencia y toma de decisiones en los adolescentes de educación básica o media, respecto al uso responsable de las TIC.

La grafica 2-10 nos permite ver la ruta de cumplimiento de cada uno de los puntos propuestos para el objetivo número 2, logrando previsualizar como se ejecutó cada aspecto planteado.

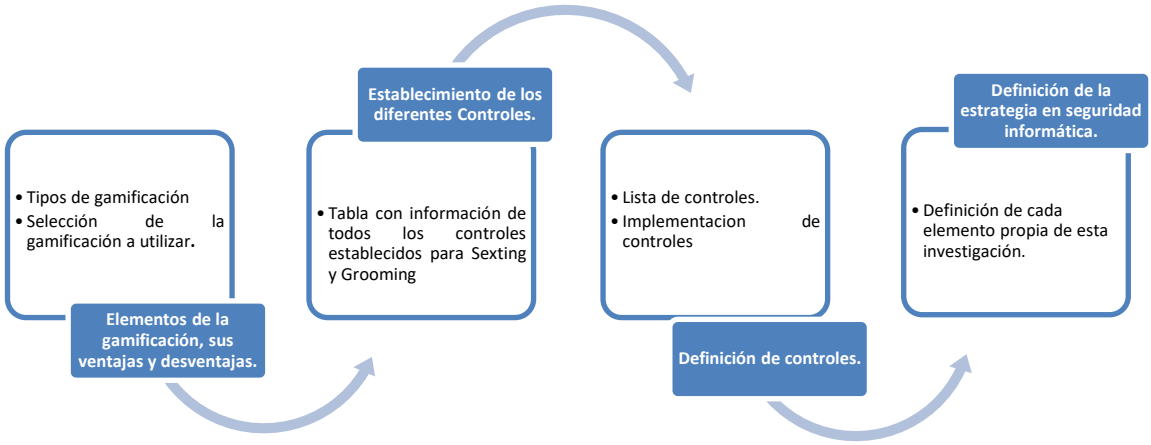

Fig. 2-10. Ruta de cumplimiento del objetivo 2. Elaboración propia.

2.2.1 Elementos de la gamificación, sus ventajas y desventajas.

A continuación, se da una descripción de los tipos de gamificación que pueden ser usados como controles de los diferentes riesgos que se establecieron previamente para el Sexting y el Grooming.

Tipos de gamificación

Gamificación educativa: Dentro de la ludificación educativa, encontramos la gamificación en educación primaria. Sin duda, se trata de un gran aliado a la hora de formar a los estudiantes en esta etapa, y es que, cuando se adquieren constantemente conocimientos de una forma divertida, logramos que los alumnos estén predispuestos a absorber más conocimientos. ¡Perfecto para que ningún estudiante se aburra en clase!

Ahora bien, se podría pensar que gamificar solo sirve para educar. La buena noticia, tanto para los docentes como para los padres, es que los juegos en contextos académicos permiten cambiar las conductas de los más pequeños dentro del aula, cuestión que también se traslada al comportamiento en casa. Los juegos de preguntas y respuestas, las mecánicas tipo Trivial, las plataformas digitales que fomentan la lectura y las aplicaciones con preguntas tipo test son solo algunos ejemplos de herramientas de gamificación que se pueden desarrollar en el aula de clases.

La gamificación en la educación secundaria logra que los alumnos asuman retos y traten de superarlos con la guía de un profesor que entiende sus inquietudes y motivaciones. Sin duda, el juego aplicado a la educación en el instituto fomenta el aprendizaje activo y consigue que el estudiante muestre interés por aquellas asignaturas que, a priori, son consideradas muy complejas o difíciles [38, 39, 41]

Gamificación empresarial: Las empresas lo tienen cada vez más claro: la gamificación empresarial aumenta el espíritu competitivo de los empleados, fortalece su compromiso con la organización, mejora la productividad, fomenta la creatividad y ayuda a que los trabajadores desarrollen habilidades concretas [40, 42]

Se trata de aplicar dinámicas y mecánicas derivadas del juego en un contexto laboral. Un claro ejemplo lo tenemos en los equipos comerciales, en donde la gamificación juega un papel fundamental a la hora de perseguir objetivos de ventas a través de empleados motivados, capacitados y bien recompensados.

Gamificación en redes sociales: Como hemos visto, la gamificación tiene múltiples aplicaciones. Comúnmente, el sector educativo y el empresarial son los que más aprovechan las ventajas de aplicar estas técnicas en sus entornos, pero hay muchas más posibilidades. En el ámbito de la salud y el bienestar, ya se empiezan a implementar técnicas de redificación que ayuden a inculcar en los ciudadanos buenos hábitos para la prevención de ciertas enfermedades. En lo social, también es posible aplicar el juego. Por otro lado, ONGs dedicadas a la protección del medioambiente han utilizado dinámicas de gamificación para transmitir el amor por la tierra y enseñar a los individuos, desde un enfoque 100% colaborativo, a reciclar y a respetar el planeta [43].

Selección de la gamificación: En conclusión, de lo anterior y para ejecución del proyecto, se selecciona y trabaja la gamificación educativa comprendiendo que el juego aplicado a la educación en el instituto fomenta el aprendizaje activo y consigue que el estudiante muestre interés por los diferentes contenidos que se le quieren enseñar, de esta manera usaremos estos criterios de gamificación atendiendo que tiene elementos propios para la población seleccionada.

2.2.2 Establecimiento de los diferentes Controles.

Después de haber realizado revisión a diferentes causas de riesgo e impactos generados para Sexting y Grooming, se establecieron algunos controles que buscan reducir los niveles de exposición, por medio de una tabla se concatenaron todas las vulnerabilidades mencionadas en las tablas 2.2 y 2.3. y para todas las vulnerabilidades a tratar se asignó un control, luego se estableció una sugerencia de estrategia de aplicación del control, usando un mecanismo de la gamificación, este mecanismo de gamificación usado contenía los siguientes criterios.

Gamificación educativa basada en juegos. Por medio de diversos y creativos juegos se les enseñara a los estudiantes un tema específico, el cual supone la definición de tareas y actividades usando los principios de seguridad de la información.

Gamificación educativa desarrollada en trivias. Conjuntos de preguntas de selección múltiple lo cual ayuda a afianzar y recordar conceptos importantes de las asignaturas en un entorno de juego y competencia.

Gamificación educativa basada video test. A partir de videos ilustrativos sobre el tema que se quiere enseñar, se realizan unos pequeños test o mini pruebas que permiten evaluar y reforzar el conocimiento de la idea impartida en el video visualizado.

Tabla 2-4

Establecimiento de los diferentes Controles. Fuente propia

Riesgo	Control	Estrategia de gamificación
Sexting	Proponer mejores prácticas en uso de cuentas de redes sociales.	Juegos de superar retos que generen información de uso de redes y uso seguro de contraseñas.
	Brindar información relevante acerca de manejo y creación de contraseñas seguras	
	Sensibilización del uso de redes públicas o abiertas.	Trivias que generen preguntas de análisis y aprendizaje respecto a temas de manejo de la información.
	Concientización de publicar en redes e internet.	
	Capacitación de manejo de internet y medio digitales.	Video y juego de preguntas sobre la prevención en las relaciones por medio de redes.
	Suministrar información general acerca del Sexting como riesgo	
	Recomendaciones acerca de establecer relaciones virtuales.	Juegos constructivos relacionado a denunciar o rechazar contactos con desconocidos.
	Informa acerca de peligros de concertar encuentros con desconocidos.	
	Sensibilización de impacto reputacional, que pueden generar riesgos asociados al Sexting.	
	Denunciar situaciones de Ciber acoso y presiones en las diferentes redes	

Grooming	Recomendaciones respecto al tiempo en internet, y prolongada navegación.	Video Test respecto a abuso del uso de internet y redes.
	Recomendaciones acerca de la información y medios que se reciben por medio de internet.	Juegos constructivos relacionado a denunciar o rechazar contactos con desconocidos.
	Educación e información respecto al Grooming.	Juegos acerca del engaño en internet y los diferentes Maneras como nos puede atacar un ciber delincuente.
	Denunciar situaciones de Ciber acoso y Grooming.	
	Sensibilizar respecto a suministrar demasiada información por medio de redes.	
	Proporcionar información de la existencia de virus, ataques y vulnerabilidades con el propósito de buscar protección.	

Nota: La tabla 2-4 nos permite tener una descripción de los respectivos riesgos establecidos sobre el Sexting y el Grooming, así como los controles sugeridos considerando las vulnerabilidades previamente identificadas en el numeral 2.2.1. Cada control busca tratar de manera general lo que conlleva a estos riesgos, además en la tercera columna de la tabla, podemos visualizar una recomendación que, a partir de la gamificación, aborda la aplicación de los diferentes controles, considerando la población de básica y media se procede a aplicar la estrategia propuesta en el presente proyecto de profundización.

2.2.3 Definición de controles.

A continuación, se brinda una descripción de los controles que se establecieron para el tratamiento de los riesgos Sexting y Grooming, cada control tiene una descripción de su aplicabilidad y como se puede ejecutar usando el mecanismo Gamificado de selección para estudiantes de educación básica y/o media, en el cual se aplicaran juegos, trivias, mini pruebas, y video test. El desarrollo usado es el propuesto por INCIBE (Instituto Nacional de ciberseguridad) de España (fig. 2-11), en la página web educativa de libre acceso https://Ciber scouts.osi.es/

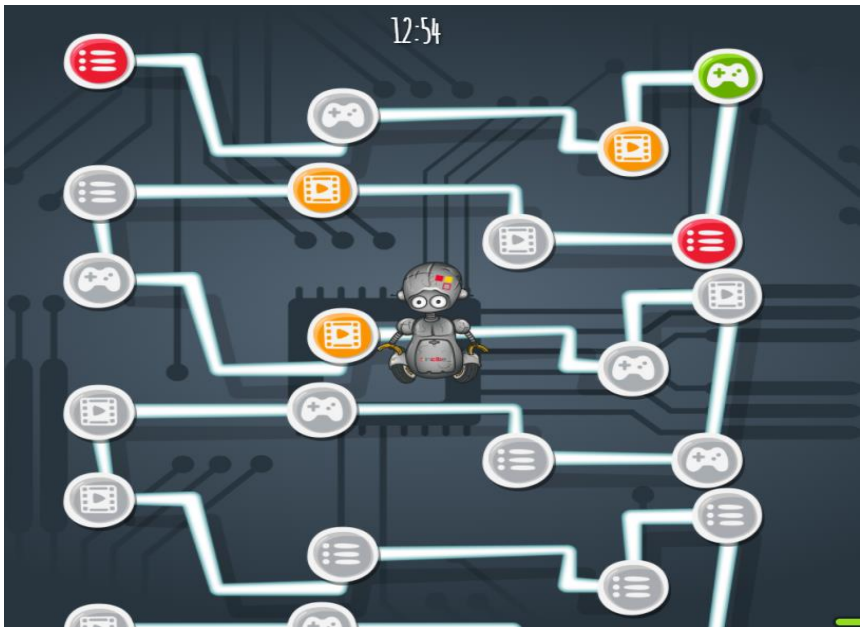

Fig. 2-11. Mapa del sitio Juego Cyberscouts.

El desarrollo del mapa de juegos es incentivado por puntos e insignias, que al final da una calificación y unas insignias que permite realizar una autoevaluación de los conocimientos recibidos durante el ejercicio, además motiva al estudiante a hacerlo mejor. Finalizada la prueba, el estudiante puede escoger repetir el mapa de juegos entre los tres diferentes niveles que para este ejercicio se proponen Fig. 2-12, siempre conservando el propósito de modelar una estrategia de seguridad informática orientada a la prevención de Ciber victimización por Sexting y Grooming.

Fig. 2-12. Niveles de juego.

Los controles seleccionados para el tratamiento del Sexting y Grooming como riesgo, se establecieron en la tabla 2.3 sumando un total de 16 controles, a continuación, una descripción la finalidad al implementar cada uno de estos controles.

2.2.3.1 Lista de controles

Control 1. Proponer mejores prácticas en uso de cuentas de redes sociales: este control busca brindar a los usuarios de redes sociales, información respecto al uso de las redes sociales y como tener mejores prácticas de uso, evitando la victimización en redes.

Control 2. Brindar información relevante acerca de manejo y creación de contraseñas seguras: por medio de este control se pretende que los jóvenes fortalezcan su conocimiento respecto al uso y configuración de las redes sociales, promoviendo hábitos preventivos.

Control 3. Sensibilización del uso de redes públicas o abiertas: Un control diseñado para sensibilizar respecto a los riesgos que puede traer el uso de redes públicas o abiertas.

Control 4. Concientización de publicar en redes e internet: Este control busca la prevención respecto a la sobre exposición en redes y los potenciales problemas que puede generar, en redes sociales.

Control 5. Capacitación de manejo de internet y medio digitales: Por medio de este control se pretende brindar información respecto al uso responsable y debido de internet y medios digitales.

Control 6. Suministrar información general acerca del Sexting como riesgo: la contextualización respecto al Sexting como riesgo, permitirá a los estudiantes concientizarse respecto a esta situación y tomar una postura ante el problema.

Control 7. Recomendaciones acerca de establecer relaciones virtuales: Este control busca la prevención en las relaciones peligrosas de los diferentes medios virtuales.

Control 8. Informa acerca de peligros de concertar encuentros con desconocidos: Por medio de este control se brinda información respecto a que puede suceder cuando un menor decide concertar encuentros de cualquier naturalidad con individuos que solo conoce por un perfil o chat, y los potenciales riesgos de victimización en los cuales puede explotar esta vulnerabilidad.

Control 9. Sensibilización de impacto reputacional, que pueden generar riesgos asociados al Sexting: Este control brinda información respecto a impactos generados al explotar vulnerabilidades asociadas al Sexting, tratando de generar una sensibilización respecto al Sexting como Riesgo.

Control 10. Denunciar situaciones de Ciber acoso y presiones en las diferentes redes: por medio de este control se promueve la denuncia y activación de mecanismos de defensa respecto a la situación de ciber acoso.

Control 11. Recomendaciones respecto al tiempo en internet, y prolongada navegación: Este control busca concientizar respecto a los prolongados tiempos de uso de internet y efectos a los jóvenes.

Control 12. Recomendaciones acerca de la información y medios que se reciben por medio de internet: Por medio de este control se informa y socializa sobre el tipo de información y contenidos que abrimos y recibimos en internet, y los efectos que podría tener la recepción de archivos con malware.

Control 13. Educación e información respecto al Grooming: Este control promueve la prevención respecto al Grooming y brinda información de situaciones alrededor.

Control 14. Denunciar situaciones de Ciber acoso y Grooming: Este control está orientado a ciber acoso específicamente como Grooming, donde se promueve que los menores denuncien actos que los podrían impactar.

Control 15. Sensibilizar respecto a suministrar demasiada información por medio de redes: la aplicación de este control es con el propósito que los estudiantes examinen y evalúen la información y excesiva publicación de datos en redes o internet.

Control 16. Proporcionar información de la existencia de virus, ataques y vulnerabilidades con el propósito de buscar protección: este control brinda información y recomendaciones respecto a virus, ataques y vulnerabilidades, con el propósito de contextualizar a los estudiantes de la exposición y como aplicar mecanismos de protección o reducción de riesgos.

2.2.3.2 Implementación de controles usando el mecanismo gamificado.

En esta etapa se realiza mención de cada uno de los controles seleccionados, y como se efectuaría la aplicabilidad de la gamificación en el cumplimiento del control, además una evidencia visual de cómo es el desarrollo usado para la ejecución e implementación del control.

Control número 1: Proponer mejores prácticas en uso de cuentas de redes sociales.

Se usa el Juego acerca de configuración de privacidad en redes sociales, donde se dan pautas de como configurar la cuenta por medio de poner todo en su lugar.

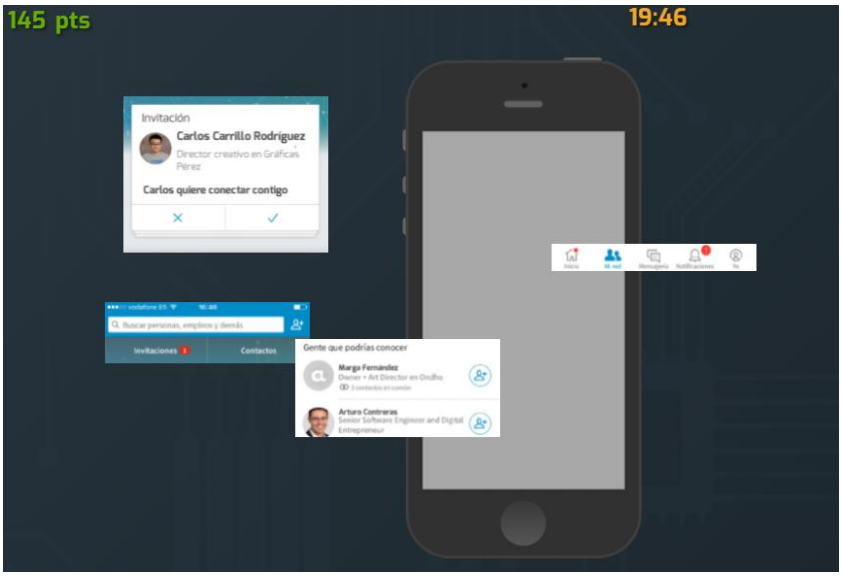

Fig. 2-13. Juego configura la privacidad.

Control número 2: Brindar información relevante acerca de manejo y creación de contraseñas seguras

Se usa una mini prueba donde se realizan preguntas con selección múltiple respecto a cómo usar las contraseñas y que son contraseñas seguras.

Fig. 2-14. Mini prueba manejo y creación de contraseñas seguras.

Control número 3: Sensibilización respecto al uso de redes públicas o abiertas.

Para este control se usa un video test donde después de visualizar un escenario animado, se realiza una prueba con el propósito de que el estudiante responda con conocimiento al usar una red pública.

Fig. 2-15. Video Test, uso de redes públicas o abiertas.

Control número 4: Concientización de publicar en redes e internet.

Se usa un juego donde se guía al estudiante a que identifique que es seguro compartir y en qué tipo de red.

Fig. 2-16. Publicar en redes e internet.

Control número 5: Capacitación de manejo de internet y medios digitales.

En este control se aplica un juego llamado compare e identifique, donde los estudiantes con un punto de comparación identifican elementos inseguros de páginas de internet, o incluso la configuración de su dispositivo.

Fig. 2-17. Manejo de internet y medios digitales.

Control número 6: Brindar y suministrar información general acerca del Sexting como riesgo

En este control se usa una mini prueba donde se realizan preguntas con selección múltiple respecto al Sexting que generen conciencia y orientación sobre el Sexting como riesgo.

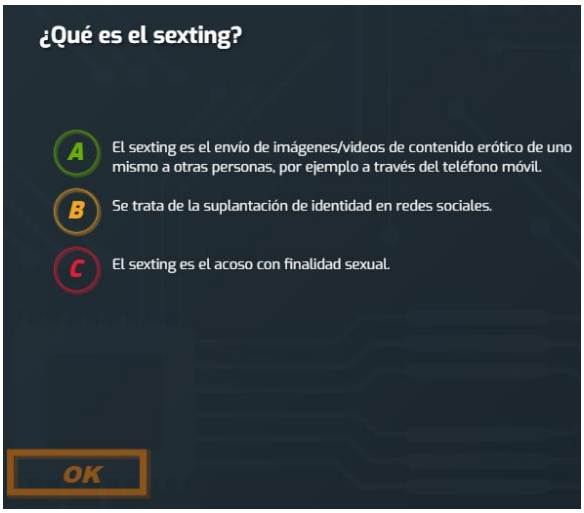

Fig. 2-18. Información general acerca del Sexting.

Control número 7: Recomendaciones acerca de establecer relaciones virtuales.

Se usa una mini prueba donde se realizan preguntas con selección múltiple sobre el manejo seguro de las relaciones y contactos en internet.

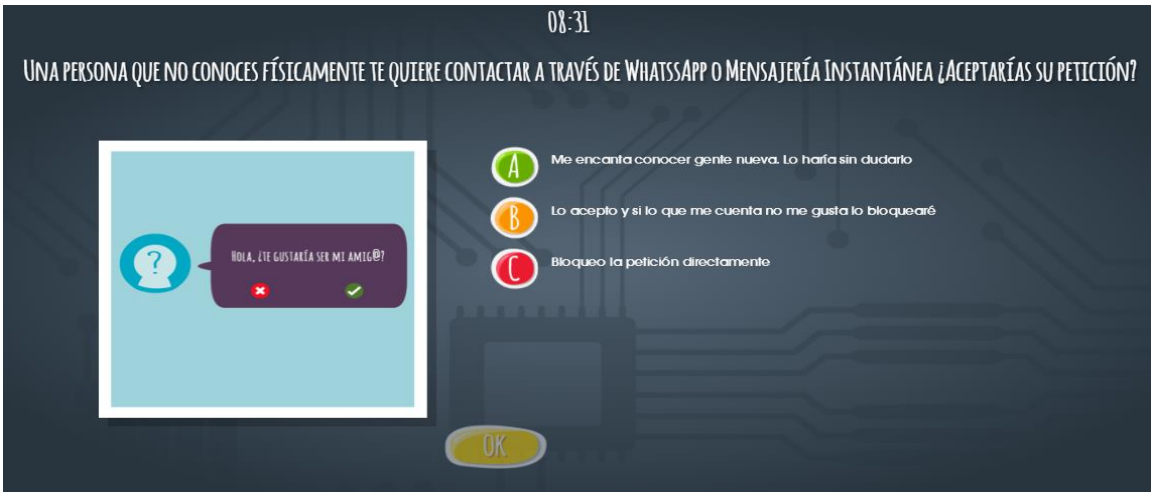

Fig. 2-19. Establecimiento de relaciones virtuales.

Control número 8: Informa acerca de peligros de concertar encuentros con desconocidos.

Se usan un video test donde se realiza preguntas con selección múltiple sobre los peligros de concretar cualquier tipo de encuentro con desconocidos o personas mayores.

Fig. 2-20. concertar encuentros con desconocidos.

Control número 9: Sensibilización de impacto reputacional que pueden generar riesgos asociados al Sexting.

En este control se usa un video test donde se realizan preguntas con selección múltiple sobre los efectos e impactos de compartir fotos o contenidos personales de carácter sexual.

Fig. 2-21. Impacto reputacional.

Control número 10: Denunciar situaciones de Ciber acoso y presiones en las diferentes redes.

Para la aplicación de este control, se usa un juego de sopa de letras y después una mini prueba donde se valida los conocimientos entregados en videos animados sobre Ciber acoso.

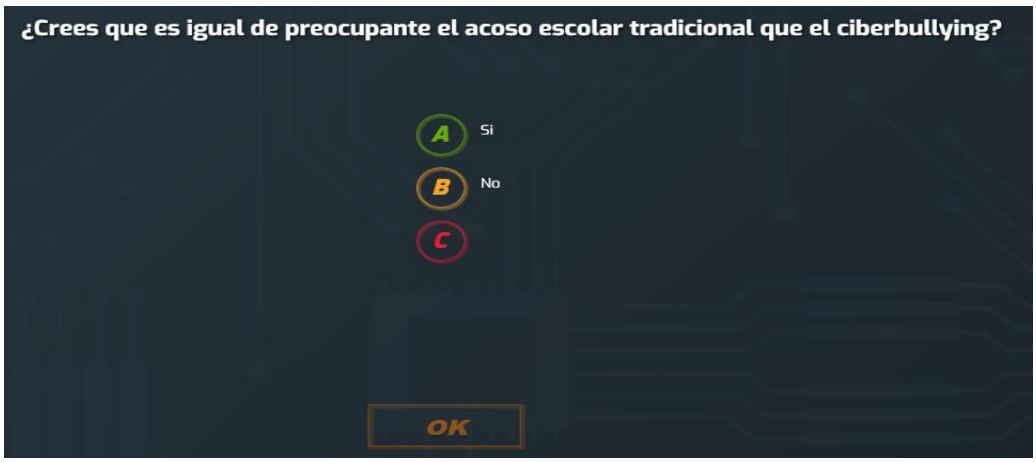

Fig. 2-22. Situaciones de Ciber acoso.

Control número 11: Recomendaciones respecto al tiempo en internet, y prolongada navegación.

En la aplicación de este control, se usa un juego de detección de intrusos y diferenciación de objetivos, después se completa con una mini prueba respecto al uso excesivo de internet.

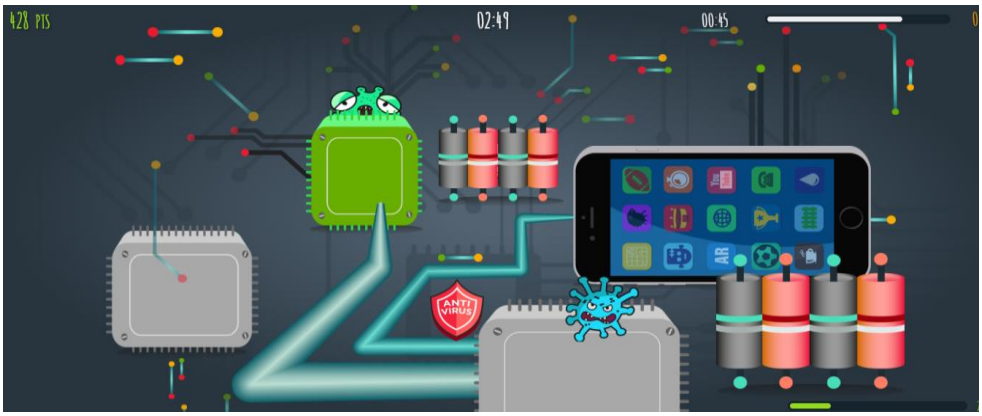

Fig. 2-23. Tiempo en internet 1.

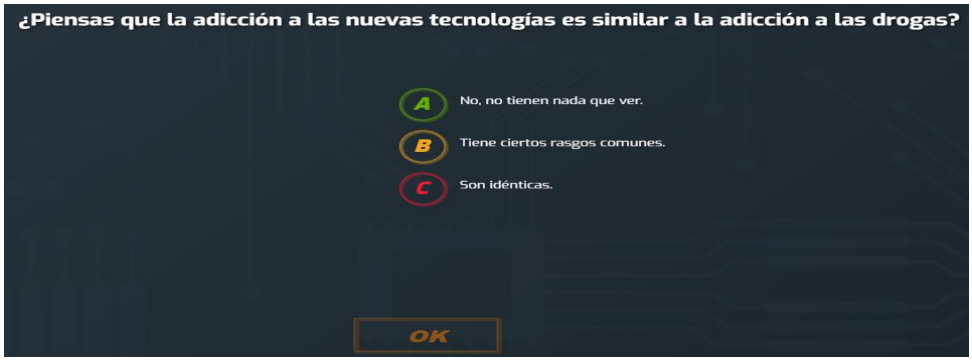

Fig. 2-24. Tiempo en internet 2.

Control número 12: Recomendaciones acerca de la información y medios que se reciben por medio de internet.

En la implementación de este control se usa un video test que permita a los estudiantes ver la animación de un escenario posible y responder como se podría actuar ante este tipo de eventos.

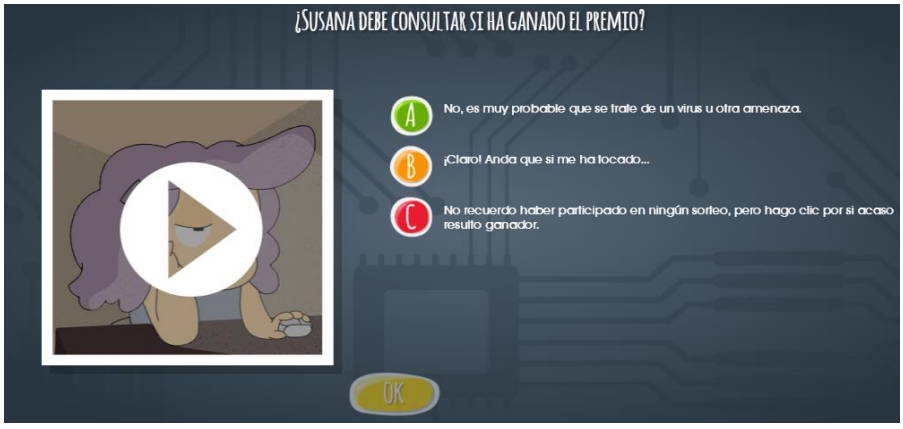

Fig. 2-25. Recibir archivos y descargas de internet 1.

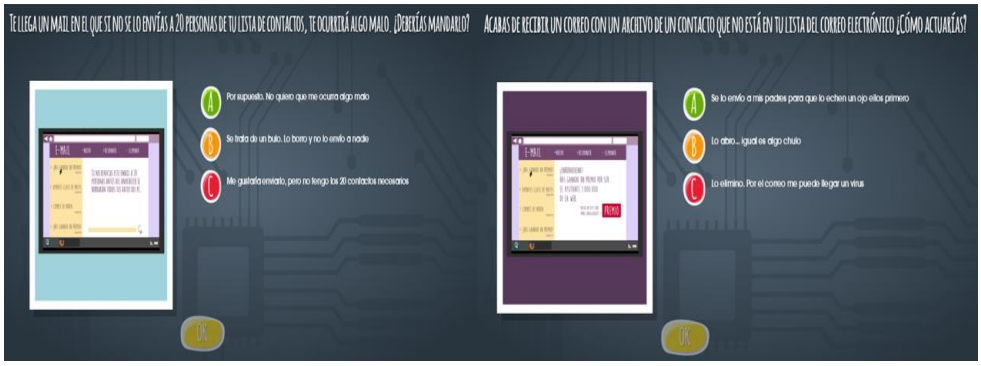

Fig. 2-26. Recibir archivos y descargas de internet 2.

Control número 13: Educación e información respecto al Grooming.

Para este control se usan dos recursos, uno es un video test donde se personifica una situación de riesgo y después una mini prueba para identificar la respuesta de los estudiantes.

Fig. 2-27. Información respecto al Grooming 1.

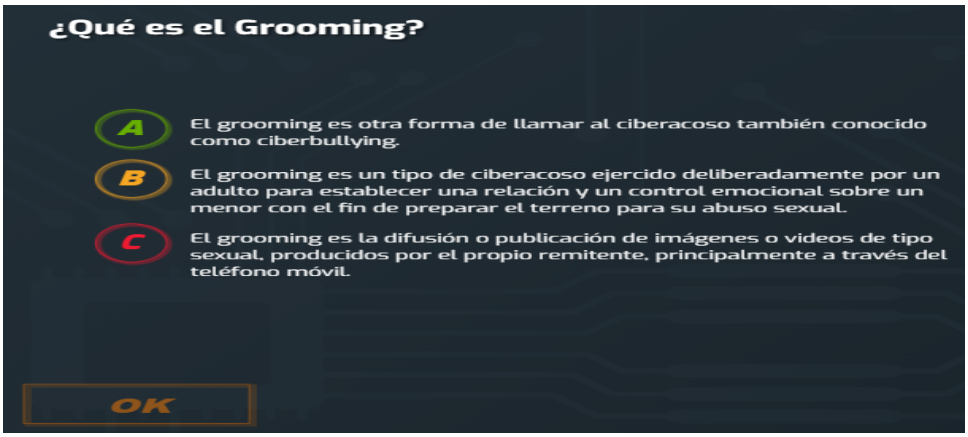

Fig. 2-28. Información respecto al Grooming 2.

Control número 14: Denunciar situaciones de Ciber acoso y Grooming.

Se usa un juego donde el estudiante debe evitar ser atacado por unos piratas que lo quieren acosar, después de jugar se visualiza video test donde el objetivo es promover la denuncia del ciber acoso.

Fig. 2-29. Denunciar Ciber acoso 1.

Fig. 2-30. Denunciar Ciber acoso 2.

Control número 15: Sensibilizar respecto a suministrar demasiada información por medio de redes sociales e internet.

En este control se implementa un juego de revisión detallada de las redes sociales donde el estudiante busca con una lupa lo que está mal en la red, y también realiza una mini prueba.

Fig. 2-31. Sobre exposición en redes 1.

Fig. 2-32. Sobre exposición en redes 2.

Control número 16: proporcionar información de la existencia de virus, ataques y vulnerabilidades con el propósito de buscar protección.

En este control, se usan dos juegos donde se ejemplifica como los virus pueden atacar los dispositivos, además, también se juega la caja que gira para que los estudiantes giren la caja y agreguen al sitio que corresponda dependiendo de la situación.

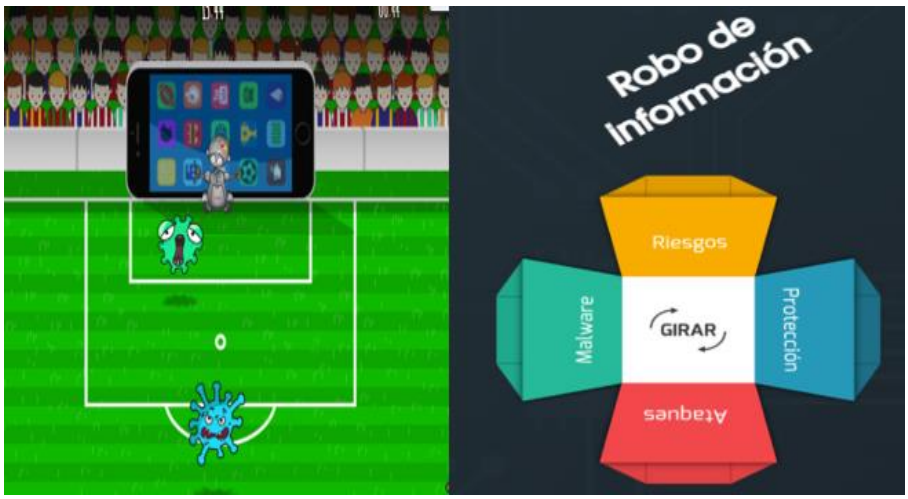

Fig. 2-33. Juegos de virus, ataques y vulnerabilidades.

2.2.4 Definición de la estrategia en seguridad informática.

La estrategia de seguridad informática que se propone para la ejecución de la propuesta investigativa contendrá los siguientes elementos.

Políticas. Plan de acción para afrontar riesgos de seguridad, o un conjunto de controles para el mantenimiento de cierto nivel de seguridad, que permita la continuidad del proyecto o los objetivos propuestos.

Seguimiento a los riesgos y sus fuentes. Se realiza una investigación exhaustiva de las diferentes fuentes de riesgo y documentación existente respecto al sexting y grooming como riesgos, así también que estrategias se han usado en su prevención, que antecedentes se tienen de implementación de controles para estos riesgos, y cuáles son las amenazas, vulnerabilidades e impactos que puedan generarse al no tratar estos riesgos.

Toma de conciencia. Se requiere contextualizar a la población acerca de las problemáticas o riesgos a tratar, partiendo de la idea que como son estudiantes de básica y media no todos tienen claro el concepto de Sexting y Grooming, y por consiguiente es necesario antes de ejecutar la estrategia de gamificación, presentar en contexto que son este tipo de riesgos y el impacto que puedan generar.

Toma de decisiones. Usando un mecanismo gamificado, se despliega la estrategia de seguridad informática donde aplicando controles previamente documentados, se realiza un tratamiento proporcionando conocimientos que lleven a la concientización respecto a la victimización por Sexting y Grooming.

Reducción de riesgos. La propuesta para reducción de riesgos está basada en la implementación de controles previamente establecidos de acuerdo con las diferentes vulnerabilidades identificadas.

Medición de estados. Se realiza una prueba inicial y una prueba después de ser desplegado la estrategia basada en gamificación, de tal manera que esto permita medir el estado inicial de la

población respecto al conocimiento de estos riesgos previamente documentados, igualmente se realiza una prueba al finalizar, con lo cual, se puede tener el estado final y el resultado de la estrategia.

Hasta este punto se ha realizado el proceso de establecimiento de los controles para las amenazas y vulnerabilidades halladas, la definición de la estrategia de seguridad informática y la selección de los criterios de gamificación que contenga los elementos para el estudio de caso, toda esta información es necesaria para poder desplegar la estrategia de prevención de ciber abusos y validar cada uno de estos elementos previamente expuestos.

2.3 Objetivo Especifico 3: Validar elementos específicos de la estrategia que apliquen para el entorno en que se hará el estudio de caso.

Para la validación de estrategia de seguridad informática, se definió un caso de estudio asociado a un centro de educación de la ciudad de Medellín, Colombia. Dicho caso de estudio cuenta con una descripción básica, demografía y aspectos relevantes de la población. Luego de definir el caso de estudio, se realizó una evaluación inicial, para lo cual, se contó con la autorización de los directivos del colegio, para luego, realizar la respectiva ejecución.

La ejecución de la validación se definió en varias fases las cuales se representan (fig. 2-33):

Fig. 2-34. Descripción de despliegue de la estrategia. Elaboración Propia.

2.3.1 Fase 1: Definición del caso de estudio:

Bajo el método de estudio de caso, se procede a desplegar la estrategia de seguridad informática en un grupo de estudiantes de la institución educativa Sebastián de Belalcázar. La institución fue creada hace 41 años aproximadamente, se encuentra ubicada en el barrio Belalcázar, en la Comuna 5, al noroccidente de la ciudad de Medellín, cerca de la Institución está la Feria de Ganado de Medellín (fig. 2-34). Cuenta con 2 sedes, una de preescolar y primaria, y otra para secundaria, cuenta con aproximadamente 520 estudiantes, 21 docentes, 1 coordinador y un rector, se trabaja jornada mañana y tarde.

Muchos de los estudiantes provienen de familias que han migrado de las distintas subregiones de Antioquia como Tarazá, Segovia, Remedios, entre otras, de la Costa Norte de Colombia y otros del departamento de Chocó.

La institución educativa es de inclusión y trabaja desde el PEI (Proyecto Educativo Institucional) por la inclusión. Las familias en su mayoría hacen parte de estratos 1 y 2, muchas de ellas trabajan en la Feria y sus anexos, otras se dedican a los oficios varios y a la construcción. Una característica de las familias de los estudiantes es que en su mayoría son familias disfuncionales donde muchos de los estudiantes se quedan al cuidado de sus abuelos o algún familiar cercano, para que sus padres o madres puedan ir al trabajo. Los estudiantes a los cuales se les realizó la prueba están en los rangos de edad de 9 y 15 años y ninguno de ellos presentan dificultades en y para el aprendizaje.

Fig. 2-35. Ubicación geográfica de la Institución.

Como punto de partida se les socializó a todos los estudiantes acerca de que trataba la prueba, se les comunicó que se realizaría una encuesta inicial con preguntas básicas acerca de tecnología y términos como Sexting y Grooming, además, se les brindó una breve definición de estos términos como riesgos, y acto seguido se realizó la prueba que contenía preguntas que se desarrollaron con la información de los riesgos obtenidos como se describe en la fase 2. Para mayor detalle de la evidencia fotográfica, ver Anexo 3

2.3.2 Fase 2. Evaluación inicial del estado de la población.

Para llevar a cabo esta actividad, se realizó una encuesta al público objetivo para lo cual, se utilizó el framework ya disponible en https://www.is4k.es/de-utilidad/test (fig. 2-35)

Fig. 2-36. Enlace para la encuesta inicial. Fuente https://www.is4k.es/de-utilidad/test.

A los estudiantes se les asignó un computador propiedad de la institución educativa y se procedió a abrir el enlace, en éste se encuentra la prueba de conocimiento con las siguientes preguntas:

1 ¿Cuáles son las principales características del ciberbullying o Ciber acoso escolar?

2 ¿El ciberbullying es menos grave que el acoso escolar tradicional?

3 ¿Sabes qué es la identidad digital?

4 ¿Crees que es lo mismo mediación parental que control parental?

5 ¿Piensas que la adicción a las nuevas tecnologías es similar a la adicción a las drogas?

6 ¿Qué es el Grooming?

7 El Sexting es una práctica que los jóvenes realizan como elemento de coqueteo o para captar la atención. ¿El principal riesgo que entraña el Sexting es?

8 ¿Crees que un buen antivirus evitará que quedes infectado?

Al finalizar la prueba de 8 preguntas, el sistema arroja un resultado entregado en porcentajes para cada estudiante, ver anexos, lo que nos permite por medio de la Tabla 2-4 gestionarlo y darle un tratamiento.

Tabla 2-5

Resultados de la evaluación de estado inicial.

numero de estudiante	resultado 1er encuesta
estudiante 1	50%
estudiante 2	50%
estudiante 3	38%
estudiante 4	50%
estudiante 5	63%
estudiante 6	75%
estudiante 7	50%
estudiante 8	38%
estudiante 9	50%
estudiante 10	63%
estudiante 11	50%
estudiante 12	50%
estudiante 13	63%
estudiante 14	38%
estudiante 15	63%
estudiante 16	38%

Después de haber realizado la prueba de 8 preguntas al grupo de 16 estudiantes, se procede a tomar la muestra general de los resultados (tabla 2-5), identificando que solo el 31.2% de los estudiantes respondió la mitad o más preguntas correctamente., y los demás que equivalen al 68.8% respondieron menos de la mitad de las respuestas correctas, este indicador no es bueno considerando que sobresale la falta de conocimiento por parte de los estudiantes encuestados respecto a conceptos básicos de seguridad, sexting y grooming.

2.3.3 Fase 3. Desplegar la estrategia de seguridad informática.

Usando todos los elementos seleccionados de gamificación, y con los controles establecidos respecto al uso de estos elementos, se procede al despliegue de la estrategia de seguridad informática, la cual tiene en consideración los controles previamente documentados para los riesgos Sexting y Grooming, haciendo uso de la aplicación pública y gratuita https://Cyberscouts.osi.es/, se le pide a la población seleccionada de estudiantes que jueguen durante 40 minutos en cada uno de los elementos que ofrece la plataforma, y que cumplan todos los retos, mini pruebas y video test, de manera didáctica, además se les permite si terminan y cumplen todos los retos que realicen nuevamente toda la actividad en niveles de dificultad más altos, considerando que la plataforma tiene Fácil, Medio y Alto según fig. 2-12.

La plataforma tiene 3 elementos distintos por los cuales los estudiantes navegarán de manera didáctica, así mismo mientras seleccionan un elemento se les estará brindando información de interés respecto a riesgos como Sexting y Grooming, y en la misma línea se estarán ejecutando los controles propuestos.

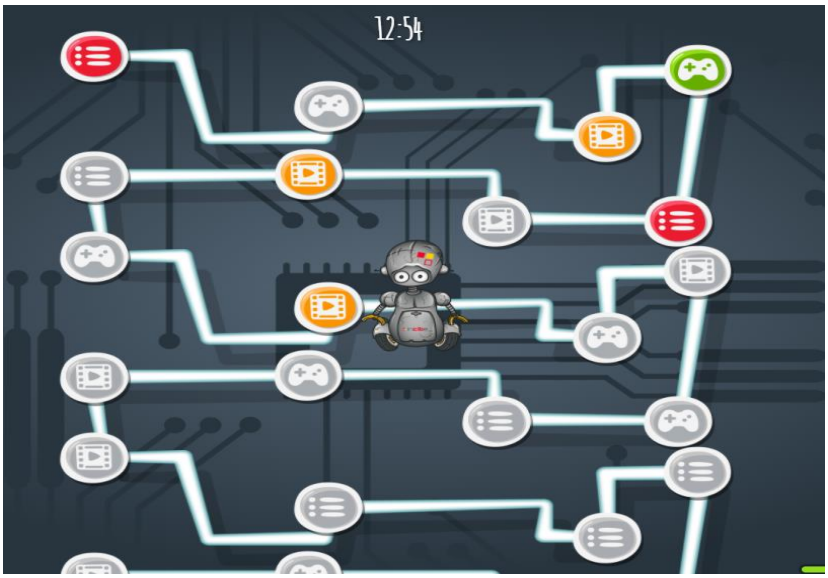

Fig. 2-11. Mapa del sitio Juego cyberscouts.

Hay tres tipos de ítem, están los juegos marcados en la imagen con verde, las mini pruebas marcados en la imagen con rojo, y los video test marcados en la imagen con amarillo. Los estudiantes podrán seleccionar en el orden que deseen cualquier ítem obteniendo una puntuación

por cada participación. Sin embargo, el propósito es que se cumplan todos los retos propuestos en el mapa como se muestra en la fig. 2-9 obteniendo una insignia y calificación de efectividad al finalizar.

2.3.4 Fase 4. Evaluación de los resultados obtenidos después del estudio de caso.

Haciendo uso de los mismos elementos que se utilizaron en la fase 1 para evaluar el conocimiento de los estudiantes, se aplicó nuevamente la encuesta en esta tercera fase. Después de haber realizado el despliegue de la estrategia gamificada, se realiza un análisis cuantitativo del estado de la población post actividades y controles, esta revisión se ejecuta a la misma población con el mismo cuestionario de la etapa inicial, las mismas 8 preguntas, tratando de facilitar el mismo escenario (fig. 2-6).

Tabla 2-6

Evaluación de estado final y tendencia.

numero de estudiante	resultado 1er encuesta	Resultado 2da encuesta	Tendencia
estudiante 1	50%	63%	
estudiante 2	50%	75%	
estudiante 3	38%	68%	
estudiante 4	50%	88%	
estudiante 5	63%	38%	
estudiante 6	75%	88%	
estudiante 7	50%	75%	
estudiante 8	38%	63%	
estudiante 9	50%	75%	
estudiante 10	63%	88%	
estudiante 11	50%	75%	
estudiante 12	50%	63%	
estudiante 13	63%	63%	
estudiante 14	38%	50%	
estudiante 15	63%	63%	
estudiante 16	38%	63%	

Nota: Los resultados de la encuesta realizada después de las actividades e implementación de los controles, permite evidenciar que el 93.7% de los estudiantes mejoraron notablemente sus respuestas, respondiendo más de la mitad de las respuestas de forma correcta.

Así mismo, se evidencia en las líneas de tendencias de la cuarta columna donde el comportamiento es ascendente, acorde a las primeras respuestas (estado inicial).

Otro resultado no menos importante se visualiza en el estudiante número 5, se evidencia que es la desviación en la muestra, ya que su desempeño bajó después de la prueba a diferencia del resto de los encuestados, en la primera encuesta el estudiante Numero 5 saco 63% de efectividad, pero después del despliegue de la estrategia de prevención y realizar todo el proceso, este mismo estudiando bajo a 38% en efectividad al momento de responder la misma encuesta.

Finalmente, y después de concluida la encuesta, se documenta la información de los resultados de cada uno de los estudiantes, evidenciando una notable mejoría en los resultados de la mayoría, comprendiendo que los conocimientos otorgados por medio del despliegue de la estrategia permitieron mejorar su percepción de los riesgos como el Sexting y Grooming.

3. Conclusiones y recomendaciones

3.1 Conclusiones

Como resultado de este proyecto de investigación aplicada, se puede concluir que las estrategias de prevención basadas en mecanismos gamificados, logran tener un impacto y respuesta positiva respecto a los objetivos propuestos y cada una de sus fases, reduciendo los posibles niveles de riesgos e impactos que se puedan presentar en los niños, niñas y jóvenes entre los 9 y 15 años de la institución de educación básica y/o media.

La estrategia desplegada en los objetivos del 1 al 3 cumplió con la propuesta del objetico general, donde por medio de un mecanismo distinto de entrega de la información, se puede lograr un aumento en la percepción, conciencia y toma de decisiones. En este sentido se evidenció en el objetivo 1 que la propuesta de exponer los orígenes de los riesgos y los impactos generados asociados el Sexting y al Grooming, mostró aspectos fundamentales para desplegar una estrategia que se ajuste a los riesgos reales que afectan a los estudiantes de educación básica y media.

Partiendo de la obtención de datos de vulnerabilidades y causas de riesgo, se logró obtener en el objetivo 2 una lista de controles a la medida de todos los riesgos, y una implementación de estos mismos controles que impactó positivamente en la población seleccionada.

En el objetivo 3, se identificó que los estudiantes son más receptivos a aprender respecto a seguridad informática y ciber victimización, al entregarles la información de una manera lúdica, con elementos que se ajusten a su nivel de conocimiento y a su vez con su entorno. El comprender el comportamiento de uso de las nuevas tecnologías por parte de los jóvenes, también permitió identificar vulnerabilidades expuestas, que explotadas pueden ultimar en riesgos como el Sexting y Grooming entre otros, además que muchos de sus impactos son poco contemplados por parte de las mismas poblaciones.

Educar de una manera lúdica a los estudiantes de básica y media respecto a seguridad informática, habilita nuevos conocimientos y mecanismos de protección frente a las amenazas constantes, estos nuevos conocimientos se convierten en información valiosa al ser evaluada, considerando que los resultados de la evaluación en algún momento son de utilidad para el planteamiento de estrategias en la prevención de ciber ataques y comportamientos que puedan generar ciber victimización.

Este trabajo permitió despejar interrogantes importantes respecto a cómo llegar y entregar una estrategia de prevención de una manera diferente y dinámica a los jóvenes de educación básica y media, además de responder a unas necesidades de capacitación; también permitió probar con un estudio de caso que la propuesta Estrategia de seguridad informática basada en gamificación, para la enseñanza en la prevención de abusos de ciber victimización por Sexting y Grooming es asertiva, positiva y replicable a otros entornos.

3.2 Recomendaciones y trabajo futuro

Se recomienda que en el proceso educativo se preste más atención y se realice un mejor trabajo respecto a la seguridad de la información, la ciber victimización y las nuevas tecnologías, considerando el alto riesgo al que están expuestos los jóvenes y adolescentes respecto al contexto de la virtualidad y las TIC.

Que el presente trabajo sea una referencia cuando se proponga realizar un tratamiento a riesgos identificados que tengan relación con el Sexting y el Grooming, además, que para otros riesgos asociados con la ciber victimización sirva como un modelo o referente en cuanto a la estrategia que se puede usar para minimizar o gestionar controles.

Fortalecer el modelo educativo cuando se refiere a la implementación y uso de nuevas tecnologías, al usar nuevas estrategias y herramientas para entregar el conocimiento. Esto es indispensable si se quiere tener una respuesta positiva o con resultados efectivos de las poblaciones con las que se desea trabajar.

Para una mejor comprensión de todos los problemas que actualmente se presentan a nivel de seguridad informática en los jóvenes de educación básica y media, se recomienda asociar e implementar nuevos lenguajes e información respecto a Sexting, Grooming, ciber victimización, entre otros, en los ambientes escolares. Hoy en día, muchos jóvenes conocen el concepto de ciber bullying, pero desconocen otros problemas asociados a la ciber victimización, lo que genera que descarten su existencia e incluso no tengan mecanismo de reacción al desconocer la presencia de estos riesgos.

Anexos

Anexo 1 – Encuesta de estado inicial.

Anexo 2 – Encuesta de estado final.

Anexo 3 – Evidencia fotográfica.

Anexo 4 – Tabulación de datos y tablas con gráficas.

Anexo 5 – informe de policía Nacional 2020

Bibliografía

[1] POLICÍA NACIONAL. (12 de 12 de 2020). policia.gov.co. Recuperado el 10 de 04 de 2021, de https://www.policia.gov.co/grupo-informaci%C3%B3n-criminalidad/estadistica-delictiva

[2] DQINSTITUT. (1 de 12 de 2020). 2020 child online safe of index. Recuperado el 07 de 04 de 2021, de https://www.dqinstitute.org/impact-measure/#impactresearch

[3] MEJÍA-SOTO, G. (2014). Sexting: una modalidad cada vez más extendida de violencia sexual entre jóvenes. Perinatología y Reproducción Humana, 28(4), 217–221.

[4] QUESADA, S., FERNÁNDEZ-GONZÁLEZ, L., & Calvete, E. (2018). Sexting in adolescence: frequency and association with victimization of cyberbullying and dating violence. Behavioral Psychology/ Psicologia Conductual, 26(2), 225–242.

[5] VILLACAMPA ESTIARTE, C., & Gómez Adillón, M. (2016). Nuevas tecnologías y victimización sexual de menores por online grooming. Revista Electrónica de Ciencia Penal y Criminología. http://hdl.handle.net/10459.1/65166

[6] GARCÍA-MALDONADO, G., Joffre-Velázquez, V. M., Martínez-Salazar, G. J., & Llanes-Castillo, A. (2011). Ciberbullying: forma virtual de intimidación escolar. Revista Colombiana de Psiquiatría, 40(1), 115–130. https://doi.org/10.1016/s0034-7450(14)60108-6

[7] MONTIEL, I., & AGUSTINA, J. R. (2019). Retos educativos ante los riesgos emergentes en el ciberespacio: claves para una adecuada prevención de la cibervictimización en menores. Revista Española de Pedagogía, 77(273), 277–294. https://doi.org/10.22550/rep77-2-2019-03

[8] BARBOSA LÓPEZ, I. M., & OJEDA BARRERA, A. E. (2018). INGENIERÍA SOCIAL UTILIZADA EN EL ABUSO DE INFANTES. Journal of Chemical Information and Modeling, 53(9), 1689–1699. https://repository.unad.edu.co/handle/10596/20334

[9] MARÍA, L., & REYES, VELÁSQUEZ. (2017). SEXTING, SEXCASTING, SEXTORSIÓN, GROOMING Y CYBERBULLYNG. EL LADO OSCURO DE LAS TICS. www.sexting.es

[10] NCMEC National Center for missing and exploited children Aiken, M., Moran, M., & Berry, M. J. (2011, September). Child abuse material and the Internet: Cyberpsychology of online child related sex offending. In 29th meeting of the INTERPOL Specialist Group on Crimes against Children, Lyons, France, September (pp. 5-7).

[11] ACUÑA NAVAS, MARÍA José.Abuso sexual en menores de edad: generalidades, consecuencias y prevención. Med. leg. Costa Rica [online]. 2014, vol.31, n.1, pp.57-69. ISSN 2215-5287.

[12] DONOSO VÁZQUEZ, T., VILÀ BAÑOS, R., Rubio Hurtado, M. J., & Prado Soto, N. (2016). Perfil de cibervictimización ante las violencias de género 2.0. Femeris: Revista Multidisciplinar de Estudios de Género, ISSN-e 2530-2442, Vol. 1, No. 1-2, 2016, Págs. 35-57, 1(1), 35–57. https://dialnet.unirioja.es/servlet/articulo?codigo=5836176&info=resumen&idioma=ENG

[13] DIAZ-VICARIO, Anna; MERCADER JUAN, Cristina y GAIRIN SALLAN, Joaquín. Uso problemático de las TIC en adolescentes. REDIE [online]. 2019, vol.21 [citado 2022-03-23], e07. Disponible en: <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1607-40412019000100103&lng=es&nrm=iso>. Epub 15-Abr-2020. ISSN 1607-4041. https://doi.org/10.24320/redie.2019.21.e07.1882.

[14] CARRERA FARRAN, X. (2019). Presentación del Monográfico Congreso Edutec 2018. Edutec. Revista Electrónica de Tecnología Educativa, 68, 2018–2020. https://doi.org/10.21556/edutec.2019.68.1409

[15] VARGAS-ENRÍQUEZ, JUAN [2015.]. Análisis de uso de la gamificación en la enseñanza de la informática. A: JENUI 2015. "Actas de las XXI Jornadas de la Enseñanza Universitaria de la Informática". Universitat Oberta La Salle ed. Andorra la Vella: Universitat Oberta La Salle, 2015, p. 105-112. URIhttp://hdl.handle.net/2117/76784 Depósito legalDL: AND.92-2015

[16] ARAUJO, V., BASTIDAS, I., & NARVÁEZ, G. (2008). La formación docente en Europa y América. Revista Unimar, 46, 33-44.

[17] BASOGAIN, X., OLABE, J., RICO, M., RODRÍGUEZ, L., & Miguel, A. (2017). Pensamiento computacional en las escuelas de Colombia: colaboración internacional de innovación en la educación. Researchgate, July, 12. http://recursos.portaleducoas.org/publicaciones/pensamiento-computacional-en-las-escuelas-de-colombia-colaboraci-n-internacional

[18] LARRAÑAGA OTAL, A. (2012). El modelo educativo tradicional frente a las nuevas estrategias de aprendizaje. Universidad Internacional de La Rioja Facultad de Educación, 69. https://reunir.unir.net/bitstream/handle/123456789/614/Larrañaga Ane.pdf?sequence=1%0Ahttps://reunir.unir.net/bitstream/handle/123456789/614/Larrañaga Ane.pdf?sequence=1&isAllowed=y

[19] DEZA VILLANUEVA, S. (2005). Factores protectores en la prevención del abuso sexual infantil. Liberabit, 11, 19–24. Recuperado 01 de abril de 2021, de http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1729-48272005000100003&lng=pt&tlng=es.

[20] FERNÁNDEZ, A. A. (2016). Menores víctimas y situaciones de victimización. VII(June), 56–74. https://dialnet.unirioja.es/servlet/articulo?codigo=5473302

[21] RÚA FONTARIGO, R., PÉREZ-LAHOZ, V., & González-Rodríguez, R. (2018). El abuso sexual infantil: opinión de los/as profesionales en contextos educativos. Revista Prisma Social, (23), 46–65. Recuperado a partir de https://revistaprismasocial.es/article/view/2764

[22] MARTÍNEZ, J. (2000). Prevención del Abuso Sexual Infantil: Análisis Crítico de los Programas Educativos. In Psykhe (Vol. 9, Issue 2, pp. 63–74). http://www.psykhe.cl/index.php/psykhe/article/view/443/422

[23] D ÁLVAREZ-GARCÍA, A DOBARRO, JC NÚNEZ - Aula abierta, 2015 – Elsevier Validez y fiabilidad del Cuestionario de cibervictimización en estudiantes de Secundaria, Facultad de Psicología, Universidad de Oviedo, Oviedo, España https://doi.org/10.1016/j.aula.2014.11.001

[24] BROWN, C. F., DEMARAY, M. K., TENNANT, J. E., Jenkins, L. N., Flynn, C., Demaray, M. K., Tennant, J. E., Brown, C. F., Demaray, M. K., Tennant, J. E., & Jenkins, L. N. (2019). Cyber Victimization in High School : Measurement , Overlap With Face-to-Face Victimization , and Associations With Social – Emotional Outcomes Cyber Victimization in High School : Measurement , Overlap With Face-to- Face Victimization , and Associations W. https://doi.org/10.17105/SPR-2016-0004.V46-3

[25] VILLACAMPA ESTIARTE, C., & CAROLINA. (2017). Predadores sexuales online y menores: grooming y sexting en adolescentes. https://recercat.cat//handle/10459.1/67854

[26] D. ESPINOSA T., J. MARTÍNEZ P., y S. Amador D., «Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2018, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC», Ing.USBMed, vol. 5, n.º 2, pp. 33–43, dic. 2014.

[27] BETANCUR, S., CARMONA, L., Contreras, R., Karam, J., Maestre, N., Romero, Y., & Uribe, S. (2014). Vídeojuegos y tic como Estrategias Pedagógicas: Formación para el uso seguro de Internet. CULTURA EDUCACIÓN Y SOCIEDAD. https://revistascientificas.cuc.edu.co/culturaeducacionysociedad/article/view/997

[28] CANTÓN MAYO, I., SANTOS, Y., & PINTO, A. (2019). Prácticas de riesgo en Redes Sociales y WhatsApp por estudiantes de educación básica secundaria. Revista Espacios, 40(23), tomado de http://www.revistaespacios.com/a19v40n23/a19v40n23p07.pdf

[29] HTTPS://WWW.HEALTHYCHILDREN.ORG/ (10/17/2016) Estar constantemente conectado: efectos nocivos del consumo mediático en los niños y adolescentes obtenido de

https://www.healthychildren.org/Spanish/family-life/Media/Paginas/Adverse-Effects-of-Television-Commercials.aspx

[30] HTTPS://WWW.ACIS.ORG.CO/ (Noviembre 19 de 2021) Niños de Latino America y uso de redes Sociales, tomado e https://www.acis.org.co/portal/content/noticiasdelsector/redes-sociales-el-45-de-los-ni%C3%B1os-en-colombia-tiene-perfil-y-el-15-de-los-padres-desconoce

[31] HTTPS://CONTIGOCONECTADOS.COM/ (Febrero de 2020) Encuesta EAFIT y TIGOUNE. Así usan los niños y jóvenes las redes en Colombia. Tomado de https://contigoconectados.com/resultados/uso-y-acceso/

[32] HTTPS://WWW.KASPERSKY.ES/ (2 de agosto de 2016) Las consecuencias del sexting tomado de https://www.kaspersky.es/blog/sexting-y-sus-consecuencias/7692/

[33] HTTPS://WWW.ICBF.GOV.CO/ (Febrero 15, 2021) Del sexting al ciberbullying y la sextorsión obtenido de https://www.icbf.gov.co/mis-manos-te-ensenan/del-sexting-al-ciberbullying-y-la-sextorsion

[34] HTTPS://CAIVIRTUAL.POLICIA.GOV.C. (24 de 10 de 2020). Peligros del Sexcam Obtenido de https://caivirtual.policia.gov.co/sites/default/files/los_riesgos_de_las_sexcam_nuevas_amenazas_en_la_web.pdf

[35] REYES RODRÍGUEZ, A. C., Vera Noriega, J. A., & Bautista Hernández, G. (2018). Desarrollo de un instrumento para medir ciber victimización en adolescentes. Informes Psicológicos, 18(2), 189–207. https://doi.org/10.18566/infpsic.20v18n2a10

[36] HTTPS://WWW.ICBF.GOV.CO/ (Marzo 18, 2021) ¿Cómo evitar ser víctima del Grooming y proteger a los menores de edad? obtenido de https://www.icbf.gov.co/mis-manos-te-ensenan/como-evitar-ser-victima-del-grooming-y-proteger-los-menores-de-edad

[37] HTTPS://WWW.EUROPOL.EUROPA.EU. (05 de 01 de 2022). Obtenido de https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

[38] BALDEÓN, J., RODRÍGUEZ, I., Puig, A., & López-Sánchez, M. (2017). Evaluación y rediseño de una experiencia de gamificación en el aula basada en estilos de aprendizaje y tipos de jugador. R. Contreras y J. Eguia, J.(Eds.), Experiencias de gamificación en aulas, 95-111.

[39] PARENTE, D. (2016). Gamificación en la educación. Gamificación en aulas universitarias, 11, 15.

[40] GARCÍA MARTÍNEZ, A., & Catalán Gil, S. Gamificación empresarial: Aplicación Volveremos.

[41] ELLES, L. M., & GUTIÉRREZ, D. (2021). Fortalecimiento de las matemáticas usando la gamificación como estrategias de enseñanza–aprendizaje a través de Tecnologías de la Información y la Comunicación en educación básica secundaria. Revista de la Asociación Interacción Persona Ordenador (AIPO), 2(1), 7-16.

[42] CLAVER-CORTÉS, E., MARCO-LAJARA, B., Úbeda García, M., García-Lillo, F., Rienda, L., Zaragoza Sáez, P. D. C., ... & Martínez-Falcó, J. (2020). El uso de la gamificación en Dirección Estratégica de la Empresa.

[43] TORTOSA, A. J. P., Sánchez, M. A., Bernal, M. J., & Gracià, V. B. Gamificación y redes sociales en el Grado en Educación: la experiencia# CCAFYDExpress.

[44] GIL VARELA, A. M. (2016). Concepciones éticas sobre el uso de las tic de los estudiantes de la Institución Educativa Octavio Harry de Medellín, grados 8° a 11°, desde el pensamiento crítico, la autonomía y la responsabilidad.

[45] BECERRA CAMACHO, J. A. (2019). *Modalidades delictivas que se desarrollan a través del sexting en Colombia: un análisis comparado con España y Estados Unidos* (Bachelor's thesis, Universidad de Ibagué.).

[46] CANO VÁSQUEZ, L. M., Rodríguez Velásquez, M., Betancur Agudelo, L., Gómez Santamaría, C., & López Arboleda, G. M. (2021). Diagnóstico de riesgos asociados al uso de internet en niños: un camino para la prevención a través de narrativas transmedia.