

Información Importante

La Universidad de La Sabana informa que el(los) autor(es) ha(n) autorizado a usuarios internos y externos de la institución a consultar el contenido de este documento a través del Catálogo en línea de la Biblioteca y el Repositorio Institucional en la página Web de la Biblioteca, así como en las redes de información del país y del exterior con las cuales tenga convenio la Universidad de La Sabana.

Se permite la consulta a los usuarios interesados en el contenido de este documento para todos los usos que tengan finalidad académica, nunca para usos comerciales, siempre y cuando mediante la correspondiente cita bibliográfica se le de crédito al documento y a su autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, La Universidad de La Sabana informa que los derechos sobre los documentos son propiedad de los autores y tienen sobre su obra, entre otros, los derechos morales a que hacen referencia los mencionados artículos.

BIBLIOTECA OCTAVIO ARIZMENDI POSADA
UNIVERSIDAD DE LA SABANA
Chía - Cundinamarca

**UN MUNDO VIRTUAL PARA LA ENSEÑANZA DE CONCEPTOS DE SEGURIDAD
INFORMÁTICA**

JUAN CAMILO GUTIÉRREZ PINZÓN

DIRECTOR: PhD RONALD SAÚL GUTIÉRREZ RÍOS

Trabajo presentado como requisito para optar el título de
Magíster en Informática Educativa

**UNIVERSIDAD DE LA SABANA
CENTRO DE TECNOLOGÍAS PARA LA ACADEMIA
MAESTRÍA EN INFORMÁTICA EDUCATIVA
CHÍA, 2016**

TABLA DE CONTENIDO

1.	RESUMEN.....	7
2.	INTRODUCCIÓN, JUSTIFICACIÓN Y PLANTEAMIENTO DEL PROBLEMA	9
	2.1 Introducción.....	9
	2.2 Justificación.....	9
	2.3 Planteamiento del problema.....	12
3.	OBJETIVOS	14
	3.1 Objetivo General	14
	3.2 Objetivos específicos.....	14
4.	MARCO TEÓRICO REFERENCIAL.....	15
	4.1 Diseño instruccional: Modelo ARCS.	15
	4.1.1 Diseño de motivación.....	19
	4.2 Teoría de Metaversos.....	20
	4.2.1 Herramientas de Modelamiento 3d - Unity.....	21
	4.3 Riesgos en las redes sociales y ataques informáticos	22
	4.3.1 Riesgos en las redes sociales.....	22
	4.3.2 Ataques informáticos	23
	4.4 Normatividad Legal	24
5.	ESTADO DEL ARTE.....	27
6.	MATERIAL EDUCATIVO.....	33
	6.1 Descripción del material educativo.....	33

MUNDO VIRTUAL DE SEGURIDAD INFORMÁTICA	2
6.2 Descripción de la estrategia Pedagógica	37
6.3 Análisis del material educativo digital	39
6.3.1 Dimensiones Evaluadas	39
7. METODOLOGÍA DE LA INVESTIGACIÓN	43
7.1 Pregunta de investigación.....	43
7.2 Tipo de estudio	43
7.3 Contexto	44
7.4 Universo, población y muestra.....	45
7.5 Instrumentos.....	46
7.6 Papel del investigador	47
8. RESULTADOS	48
8.1 Categorías de análisis.....	49
8.2 Red Semántica	51
8.3 Resultados por categoría de análisis.....	52
9. CONCLUSIONES	63
10. PROSPECTIVA Y RECOMENDACIONES	66
CRONOGRAMA.....	67
BIBLIOGRAFÍA	68
ANEXOS.....	71
Anexo 1: Formato de evaluación del material educativo.....	71
Anexo 2: Story Board	76
Anexo 3: Formato de Diario de campo.....	81

Anexo 4: Cuestionario.....	82
Anexo 5: Entrevista.....	83
Anexo 6: Cuadro de comentarios de segmentos de análisis de categorías.	84
Anexo 7: Respuestas Cuestionario.....	86
Anexo 8: Grabación incorporada en el diario de campo.....	92
Anexo 9: Formato de Autorización.....	94

Lista de Tablas

Tabla 1: Tabla de referencias de recursos utilizados..... 40

Lista de ilustraciones

Ilustración 1: Modelo ARCS (Horner, 2016)	15
Ilustración 2: Ataques informáticos incluidos en el mundo virtual.....	23
Ilustración 3: Horizon Report 2016 (New Media Consortium [NMC], 2016).....	27
Ilustración 4: Punto de partida tour virtual.....	34
Ilustración 5: Ingreso a los escenarios	34
Ilustración 6: Objetivos, instrucciones de uso	35
Ilustración 7: Mapa del sitio	35
Ilustración 8: Escenario de Riesgos en las Redes Sociales.....	36
Ilustración 9: Escenario de Ataques Informáticos.....	36
Ilustración 10: Conferencias TED.....	37
Ilustración 11: Escenario TED.....	37
Ilustración 12: Fases de la Implementación del Material Educativo	38
Ilustración 13: Opciones de configuración gráfica y controles	39
Ilustración 14: Fotos de Implementación del material educativo.	48
Ilustración 15: Fusión de Categorías de Análisis	49
Ilustración 16: Red Semántica	51
Ilustración 17: Gráfica de la categoría Percepción.....	53
Ilustración 18: Gráfica de la categoría Percepción.....	53
Ilustración 19: Gráfica de la categoría Confianza	56
Ilustración 20: Gráfica de la categoría Confianza	56
Ilustración 21: Gráfica de la categoría Atención	58

Ilustración 22: Gráfica de la categoría Atención 59

Ilustración 23: Gráfica de la categoría Relevancia..... 61

Ilustración 24: Gráfica de la categoría Relevancia..... 61

Ilustración 25: Cronograma 67

1. RESUMEN

Se incorporaron estrategias innovadoras y didácticas para el aprendizaje de conceptos de seguridad informática y riesgos en redes sociales, por medio de un tour virtual creado en Unity, utilizando un diseño instruccional basado en el modelo motivacional. Su objetivo fue describir la percepción del estudiante acerca de un material educativo basado en un mundo virtual que permitió el aprendizaje sobre riesgos en las redes sociales, los ataques informáticos y cómo prevenirlos. La investigación fue de tipo cualitativa y se utilizó un marco de estudio de caso.

Se aplicaron tres instrumentos a una muestra de 16 estudiantes de octavo semestre de la Universidad de Cundinamarca: cuestionario, entrevista y diario de campo, para obtener los datos, determinar los hallazgos y posterior análisis de las categorías: percepción, atención, confianza y relevancia. Se encontraron resultados tecnológicos en interactividad y pedagógicos de eficacia, temática y usabilidad.

ABSTRACT

The project aims is contribute on the incorporation of innovative teaching and learning concepts for computer security and risks in social networks through a virtual tour created in Unity; based on the instructional motivational model. The objective is to describe the student's perception about an educational material based on a virtual world that allows learning about risks in social networks, cyber-attacks, and how to prevent them. Qualitative research and study case framework were used.

To obtain data, determine findings, and subsequent analysis, three instruments, were applied to a sample of sixteen students of eighth university of Cundinamarca level: questionnaire, interview and journal. Categories on perception, attention, confidence and relevance were assessed. Interactivity and technology in pedagogical efficacy results, thematic and usability they found.

PALABRAS CLAVE

Tour virtual, Unity, percepción, riesgos en redes sociales, ataques informáticos, modelo motivacional.

2. INTRODUCCIÓN, JUSTIFICACIÓN Y PLANTEAMIENTO DEL PROBLEMA

2.1 Introducción

Las herramientas tridimensionales en los mundos virtuales no son nuevas. Lo importante en el tema es abordar proyectos en el que se evidencie el desempeño de ellas con enfoque educativo para lograr que los participantes transformen el conocimiento acerca de la informática, mediante la didáctica del tour en un mundo virtual como estrategia innovadora.

El propósito del proyecto es describir la percepción de los estudiantes acerca del material educativo, el mundo virtual, en el aprendizaje de los riesgos en las redes sociales y ataques informáticos y la eficacia de la herramienta para los docentes desde el punto de vista tecnológico y pedagógico, como también analizar el aprendizaje del estudiante, y todo enmarcado dentro del concepto de las TIC.

El proyecto se enfoca en tres ejes fundamentales de acuerdo con el modelo TPACK - Tecnología, Pedagogía y Contenido (Koehler y Mishra, 2009). El primero, se refiere a la mediación tecnológica, el metaverso, que fue desarrollado con la herramienta Unity.

El segundo eje, al diseño instruccional aplicado en el recurso educativo digital, el modelo motivacional ARCS (Atención, Relevancia, Confianza y Satisfacción) del profesor John Keller.

Y el tercero, el eje disciplinar, que tiene relación con los riesgos en las redes sociales y conceptos de seguridad informática.

2.2 Justificación

La comunidad educativa en general vive una nueva forma de comunicación en función de los avances en las TIC. Esta situación la han consignado muchos autores en diversas formas, por

ejemplo: “nuestros alumnos viven una nueva era comunicativa. El desarrollo de la tecnología ha permitido que los teléfonos celulares, la computadora, Internet, etc., sean parte inherente de la forma en que nos comunicamos e interactuamos” (Piscitelli, 2009). Como consecuencia, los docentes deben incluir en el día a día de su ejercicio profesional estas tecnologías para estar al unísono con los estudiantes y utilizarlas como herramientas estratégicas en el logro de los procesos educativos, que constituye el porqué de esta investigación.

Es necesario que la práctica pedagógica disponga de nuevas estrategias didácticas para el logro del aprendizaje, Naya, López e Ibáñez (2012) afirman:

“A diferencia de los sistemas TIC tradicionales, la educación dentro de un entorno inmersivo introduce a niños, adolescentes y jóvenes al ambiente familiar de los videojuegos, acercándoles el conocimiento de una forma diferente, motivando el aprendizaje a través de actividades lúdicas como mini-juegos, lecciones interactivas y experimentos vivenciales, logrando de esta manera, mantener de manera continuada la atención de los estudiantes”. (p.126)

En la actualidad en la Universidad de Cundinamarca extensión Chía, existen algunos ambientes de aprendizaje, basados en la plataforma Moodle, pero ninguno acerca de seguridad informática y en general los materiales educativos son mínimos por no decir ausentes.

Teniendo en cuenta la importancia que tienen las redes sociales y la “huella pedagógica” y cultural que estas generan en la sociedad, adquiere relevancia el proceso de investigación para identificar la efectividad de materiales educativos innovadores en el aprendizaje de algunos conceptos identificados: *sexting*, envío de contenidos eróticos o pornográficos, Davidson (2015), *grooming*, acciones realizadas por un adulto con el objetivo de conseguir la amistad de un menor de edad, UNICEF (2014).

Otro aspecto relevante tiene que ver con algunos conceptos de seguridad informática, como por ejemplo el *phishing*, suplantación de identidad (Pere y Oliver, 2015), *hoax*, mensajes falsos (Shambhu, 2016) y *spoofing*, técnicas de suplantación de identidad son algunos tipos de ataques informáticos los cuales amenazan la información personal, que pueden afectar la intimidad, la privacidad o generar pérdidas económicas, y no solo a los jóvenes sino a la población en general (Pere y Oliver, 2015). Además, se busca fundamentar buenas prácticas en los estudiantes y el uso de políticas existentes para minimizar los riesgos presentes en las redes sociales y las amenazas mencionadas.

Para el presente estudio se contó con la participación de los estudiantes de octavo semestre de Ingeniería de Sistemas de la universidad de Cundinamarca, que poseen conocimientos en el manejo de algunas herramientas informáticas y de programación de computadores, entre otros; en edades entre los 21 y 35 años y quienes hacen uso del Internet e ingresan a diario a las redes sociales, como ejemplo, Facebook, además, en el momento de la implementación del tour virtual desconocían la temática.

El propósito es desarrollar un mundo virtual como herramienta pedagógica para el aprendizaje de los conceptos antes enunciados, sus riesgos, cómo prevenirlos y realizar una investigación enfocada principalmente en la percepción del estudiante acerca de las características técnicas y pedagógicas del material educativo como herramienta en el proceso de aprendizaje. Por tal razón, se requiere implementar materiales educativos cuya temática sea el correcto uso de las redes sociales, el manejo de la información que se publica en Internet y los riesgos, amenazas y vulnerabilidades que atentan contra la información personal, para brindar las condiciones, los contenidos y las herramientas adecuadas en el aprendizaje de seguridad informática. Dichos

conocimientos podrán ser utilizados por el estudiante para proteger su información personal y en su ejercicio profesional.

2.3 Planteamiento del problema

La problemática de la investigación se divide en dos focos, primero, el desconocimiento de conceptos básicos de seguridad informática por parte de los estudiantes de Ingeniería de Sistemas de la Universidad de Cundinamarca y segundo, la ausencia de materiales educativos innovadores para el aprendizaje de dichos conceptos en la misma.

Con respecto al primero, en julio del año 2013, la compañía internacional de seguridad RSA que presta sus servicios al 70 por ciento de la banca en Colombia, dio a conocer un estudio en el cual Colombia ocupa el quinto lugar en la lista de los países más atacados en la “nube” y es el segundo país latinoamericano donde más fraudes virtuales se realizaron, superado solo por Brasil (Kessem, 2012). Por lo tanto, para todas las personas es indispensable tener un conocimiento mínimo acerca de seguridad informática, especialmente en una sociedad de la información (Voutssas, 2010). En la actualidad, existen una gran variedad de productos y servicios disponibles en la web que definen la forma en que los seres humanos, se comunican, se divierten, estudian, trabajan, etc., quedando en riesgo la información personal de cada usuario.

Igualmente, en un estudio realizado por Pew Research Center, sólo en Estados Unidos el 4% de los jóvenes entre 12 y 17 años enviaron una imagen desnuda, total o parcialmente a otra persona a través de sus teléfonos móviles (Pew Research Center, 2009). En muchos de los casos existe un desconocimiento de los riesgos mencionados y al ser víctimas de alguno de ellos no saben qué acciones tomar para minimizar las consecuencias.

El segundo foco de la problemática lo constituye la ausencia de materiales educativos en el programa de Ingeniería de Sistemas de la Universidad de Cundinamarca, donde el investigador pudo constatar el déficit de este tipo de recursos mediante el ejercicio de su actividad docente.

Así mismo, los programas académicos de la Universidad de Cundinamarca - extensión Chía, no disponen de Recursos Educativos Digitales que permita a los estudiantes tener conocimiento de los riesgos en las redes sociales y de conceptos de seguridad informática. Además, se observa que, en la mayoría de los métodos, las estrategias y las herramientas utilizadas en el proceso académico no han sido diseñadas en función de la motivación del estudiante, como tampoco en su percepción y/o interés.

En este caso se hace necesario que en los programas relacionados con informática o sistemas incluyan objetos de aprendizaje ya sean materiales o ambiente educativos con intencionalidad pedagógica que logren el aprendizaje de núcleos temáticos en relación con los riesgos en las redes sociales y conceptos de seguridad informática y proporcionen a los estudiantes instrumentos para alcanzar algunas buenas prácticas en el uso de estas tecnologías.

Lo anterior conlleva a plantear la siguiente pregunta de investigación:

¿Cuáles son las características desde el punto de vista tecnológico y pedagógico que se observan en un mundo virtual de conceptos de seguridad informática en función de la percepción del estudiante como estrategia de aprendizaje?

3. OBJETIVOS

3.1 Objetivo General

Describir la percepción del estudiante en función de las características tecnológicas y pedagógicas de un mundo virtual de conceptos de seguridad informática como estrategia de aprendizaje en estudiantes de octavo semestre de Ingeniería de Sistemas.

3.2 Objetivos específicos

- a. Indagar las características tecnológicas relacionadas con la interactividad y las pedagógicas de eficacia, temática y usabilidad que presenta el material educativo.
- b. Describir las interacciones que se generan entre los estudiantes y el material educativo.
- c. Analizar el tour virtual como estrategia pedagógica en la enseñanza de conceptos de seguridad informática en función de la percepción del estudiante.

4. MARCO TEÓRICO REFERENCIAL

De conformidad con el modelo TPACK (Koehler y Mishra, 2009), se definieron tres ejes teóricos como fundamento para la presente investigación: Pedagogía, Tecnología y Contenido. En el primero se exponen las características del modelo de diseño instruccional motivacional ARCS (por las siglas Atención, Relevancia, Confianza, Satisfacción. Keller, 2009) implementado en el material de aprendizaje. Después se hace un recorrido acerca del concepto de metaverso y su aplicación en el sector educativo y, por último, se indagan los conceptos de riesgos en las redes sociales y los ataques informáticos a incluir en el recurso educativo digital, el mundo virtual.

4.1 Diseño instruccional: Modelo ARCS.



Ilustración 1: Modelo ARCS (Horner, 2016)

El modelo ARCS (Attention, Relevance, Confidence, Satisfaction, ilustración 1) fue ideado por el profesor John M. Keller (2009), de la Universidad Estatal de Florida. Dicho modelo se basa en la motivación para el logro del aprendizaje en el que “La motivación se refiere ampliamente lo que la gente desea, lo que eligen hacer y lo que se comprometen hacer. Las investigaciones

intentan explicar la preocupación profundamente arraigada entre la gente de por qué hacemos las cosas que hacemos” (p.3). El modelo busca estrechar los lazos entre el sentir de los estudiantes y el conocimiento para superar los obstáculos y lograr las metas.

Es un modelo de aprendizaje motivacional donde John Keller argumentó que las expectativas son el motor que anima a las personas a un proceso formativo, donde la motivación está asociada a la tarea a realizar y el éxito esperado con su logro (Ibid). En el proceso de enseñanza, la formación será motivadora si el aprendizaje tiene sentido y es significativo para el estudiante. Dentro de este modelo se tienen 4 principios para estimular y mantener en el alumno la motivación durante el proceso de aprendizaje, estos son:

Atención. Es el primer elemento a implementar en un proceso educativo y se estimula la curiosidad de diversas formas como lo son preguntas o problemas. López (2005) define la atención en el modelo ARCS así:

Son el conjunto de iniciativas a emprender para despertar y mantener la curiosidad y el interés de los aprendices. Para ganar y sostener la atención debe mantenerse viva la curiosidad de los aprendices. Además, los materiales a usar por los aprendices deben ser atractivos, bien estructurados y con una maquetación y grafismo que faciliten su lectura y comprensión. (p.156)

Es posible implementar estrategias para conservar la atención implementando diferentes recursos como videos, juegos, retos, etc., sin que lleguen a convertirse en distractores. Por otra parte, existe una estrecha relación entre la atención y el interés del estudiante. Reigeluth (2013) afirma: “las teorías de aprendizaje incluyen algunas hipótesis sobre el interés. Un estudiante tiene que al menos prestar atención a un estímulo para que ocurra el aprendizaje. Como una variable de motivación, el interés abarca varias teorías de la curiosidad” (p.398). En la presente investigación se abordan temáticas que son del interés de los estudiantes, por citar alguna, las redes sociales, además de incorporar una herramienta innovadora, el mundo virtual.

Relevancia. Este principio es llamado también pertinencia y su objetivo es incrementar la motivación en el estudiante. López (2005) afirma:

Son las actividades orientadas a vincular el aprendizaje a las necesidades e intereses de los aprendices. No siempre es fácil descubrir la relevancia de los aprendizajes. Una manera de resolver esta cuestión es vincular los contenidos de aprendizaje a cuestiones con las cuales esté familiarizado el aprendiz. Keller afirma que la mejor manera de asegurar la relevancia es relacionar claramente los contenidos de aprendizaje con contenidos ya sabidos y con la experiencia del aprendiz. Para ello el formador puede usar metáforas y analogías a través de las cuales el aprendiz comprenderá los nuevos contenidos de aprendizaje. (p.156)

Como estrategias principalmente se usan ejemplos concretos del tema, abarcando necesidades, experiencias y/o necesidades. Es importante que los alumnos encuentren significado en los recursos utilizados.

Confianza. Son las estrategias que tiene como objetivo brindar a los estudiantes una perspectiva objetiva acerca de la posibilidad del logro del aprendizaje. Generar en los estudiantes una expectativa positiva sobre el éxito en el aprendizaje. Lima y Capitão (2003) enuncian el principio de confianza así:

Las tácticas pertinentes, a desarrollar en los alumnos la sensación de que son capaz de realizar con éxito las tareas de aprendizaje incluyen: objetivos de la instrucción clara, no ambigua. La educación con niveles progresivos de dificultad. Proporcionar a menudo la naturaleza de la respuesta o confirmación correctiva. (p.106)

Si la dificultad en las actividades incluidas en el material educativo es demasiado alta, la motivación en los alumnos disminuye, en contraste con la mejora del desempeño que busca este principio.

Satisfacción. La motivación es un término paralelo con el éxito de un aprendizaje gratificante o agradable, al respecto, Lima y Capitão (2003) afirman:

Asignar un premio intrínseco o extrínseco al esfuerzo desarrollado por el estudiante en el aprendizaje. La satisfacción es un componente clave en la motivación. Si los estudiantes se sienten bien con los resultados de aprendizaje será entonces motivados para aprender. Estos son algunos ejemplos de las estrategias clave en la promoción:

Las recompensas intrínsecas:

- Proporcionar ayuda inmediata después de hacer una acción incorrecta.
- Proporcionar una respuesta positiva después de completar una tarea con éxito.
- Hacer el trabajo de los estudiantes en la Web para ser compartida por otros.
- Las recompensas extrínsecas:
- Calificaciones obtenidas en el aprendizaje, emisión de certificados, etc. (p.107)

El premio otorgado a los estudiantes depende de varios factores, como la edad de los estudiantes, intereses, etc., y siempre debe ir acompañado de un proceso de realimentación por parte del docente y/o refuerzo según se requiera.

Así mismo, el modelo ARCS sugiere incorporar algunas estrategias para el logro de la implementación de cada una de sus ejes. Kovalchick y Dawson (2003) las enuncian de la siguiente forma:

Atención, variar los métodos, medios, actividades y materiales utilizados durante la instrucción, use preguntas difíciles, problemas realistas, o representar situaciones para estimular la curiosidad de los alumnos. Pertinencia, Incluir ejemplos que son familiares para los estudiantes, mostrar a los estudiantes cómo el contenido se relaciona con alguna experiencia anterior, y mostrar a los estudiantes cómo el contenido se relaciona con alguna necesidad personal o meta. Confianza, proporcionar a los estudiantes con requisitos claros para el curso asignaciones, proporcionar a los estudiantes oportunidades para ejercer el control sobre ¿Qué y cómo aprender? y proporcionar a los estudiantes con ejercicios o tareas que poco a poco van aumentando en dificultad. Satisfacción, fomentar el disfrute de los estudiantes de aprender por su causa, proporcionar a los estudiantes con retroalimentación positiva y dotar al alumno de elogio verbal y otras formas de recompensa tangible. (p.35)

De acuerdo a lo anterior, todo material educativo debe disponer de recursos de diferentes tipos y se debe realizar una selección apropiada de cada uno de ellos conforme con las estrategias mencionadas, para generar y conservar la motivación y el interés en los estudiantes.

4.1.1 Diseño de motivación

Para el éxito en un proceso educativo, debe existir en el estudiante la voluntad de aprender, concepto que está ligado con la motivación. Por lo anterior es necesario que el diseño instruccional del material educativo incluya en sus recursos elementos que se enfoquen en este concepto. Así, el diseño motivacional se refiere a las estrategias, procesos y recursos que hagan que el material sea atractivo (Keller, 2016). El diseño de motivación debe ser un parámetro a tener en cuenta en el desarrollo de los recursos en el material educativo.

Por otra parte, la eficiencia es una dimensión relacionada con la permanencia de la motivación en el estudiante y su afectación es desde un punto de vista negativo. “Si un evento de instrucción hace un uso ineficiente del tiempo, los recursos pueden ser aburridos para el público. Sin embargo, la eficiencia de la entrega no se añade al interés intrínseco de los estudiantes en la situación” (Keller, 2016). Lo anterior justifica la observación del tiempo en el uso de los recursos al implementar el material educativo.

Existen varios modelos de motivación, según John Keller en la página oficial del modelo ARCS (Keller, 2016), afirma:

Se pueden clasificar en los siguientes cuatro grupos, los tres primeros se fundamentan en las teorías psicológicas de la conducta humana. Se pueden clasificar como teorías centradas en la persona, teorías centradas en el medio ambiente, y las teorías de interacción. El cuarto grupo es más pragmático o pedagógico, incluye modelos de ómnibus que incorporan tanto el diseño instruccional y diseñar estrategias de motivación. Estos modelos tienden a crecer fuera de soluciones a los tipos específicos de problemas de instrucción.

El enfoque o modelo a seguir en el recurso educativo digital, depende del objetivo pedagógico y la intencionalidad del docente, porque es posible que dicho recurso sea atractivo para los usuarios, pero no efectivo en términos de aprendizaje, de allí la importancia de la selección del tipo de diseño motivacional.

4.2 Teoría de Metaversos

El término metaverso fue utilizado por primera vez por el profesor de la Universidad de Indiana Neal Stephenson, en su novela Snow Crash (1992), y se refería a espacios de trabajo tridimensionales. “Un mundo virtual, (también conocido como mundo 3D, entorno inmersivo o el genérico metaverso) se define como un entorno gráfico que se materializa en la pantalla del ordenador del usuario conectado” (García y González, 2011). Los mundos virtuales se observan en los videojuegos, como su principal fuente de aplicación, sin embargo, es posible aplicarlos en diferentes áreas del conocimiento, en diseño, en estudios sociales, etc.

Es importante mencionar las características de los metaversos, porque a partir de estas se vislumbran los aspectos a tener en cuenta en el diseño del recurso educativo digital. Sin embargo, es preciso aclarar que el material educativo de esta investigación es un tour virtual donde la interacción del estudiante es con los recursos y los elementos del material educativo y no entre usuarios. Al respecto Castronova (2001) menciona:

Existen tres características fundamentales de los metaversos:

- Interactividad. El usuario es capaz de comunicarse con el resto de usuarios y de interactuar con el metaverso. Esto implica que sus comportamientos pueden ejercer una influencia sobre los objetos y sobre los comportamientos y opiniones de otros usuarios, influencia que también puede ser recíproca.
- Corporeidad. Los usuarios están representados por avatares y están limitados por una altura y un peso considerables. La corporeidad consiste en la presencia de ese avatar sobre ese espacio que también posee ciertos límites, ya que está sometido a ciertas leyes y tiene recursos limitados.

- Persistencia. Esto significa que el programa sigue funcionando y desarrollándose a pesar de que algunos o todos sus miembros no estén conectados. Además, las posiciones en las que se encontraban los usuarios al cerrar sus sesiones, así como sus conversaciones, objetos de propiedad, etc., siempre son guardados, lo que permite recuperarlos cuando nos volvamos a conectar. El término metaverso suele emplearse como sinónimo de mundo virtual tridimensional. (p. 6)

Algunos tratadistas enmarcan los metaversos con el proceso educativo así: “En los últimos años, la pantalla de ordenador se ha venido utilizando como espacio para la educación, es decir, como esa tele-puerta o tele-ventana que nos permite acceder a las aulas de muros pixelados donde se desarrolla una parte importante del proceso de enseñanza y aprendizaje en la sociedad de la información y del conocimiento” (Márquez, 2010). Los metaversos son un espacio de interacción social de los seres humanos, utilizando un ícono o avatar, inclusive llegan a tener una inmersión prolongada como en el caso de second life, que es un metaverso online con miles de usuarios.

Los metaversos son un método novedoso de aprendizaje que ofrece ventajas frente a otras estrategias pedagógicas: “Las principales ventajas que ofrecen los mundos virtuales son: la experiencia que proporcionan, ya que estar e interactuar en un mundo virtual es lo más parecido a lo que se puede sentir en el mundo real que simula” (Monterroso y Romero, 2011). Lo anterior, fundamenta la creación de los diferentes escenarios sobre un mundo virtual de una isla simulando un ambiente de aislamiento para lograr la atención en los usuarios.

4.2.1 Herramientas de Modelamiento 3d - Unity

Los mundos virtuales pueden ser creados a partir de diferentes herramientas que están disponibles en el mercado, tanto libres como propietarias (es decir de pago). El material educativo se desarrolló con el software Unity que es una plataforma de desarrollo de videojuegos, según la página oficial (Unity, 2016) “es un ecosistema de desarrollo de juegos, es

un poderoso motor de renderizado totalmente integrado con un conjunto completo de herramientas intuitivas y flujos de trabajo rápido para crear contenido 3D interactivo”. La versión 5, tiene dos tipos de licenciamientos, la licencia de Unity Pro se adquiere en su totalidad o tiene una versión de prueba limitada. Incluye tutoriales, ejemplos de proyectos, y en Internet están disponibles diversos materiales para el aprendizaje de la herramienta.

Existe un servicio llamado Unity Asset Store donde los usuarios pueden acceder a la colección de paquetes de Assets (o elementos) por categorías como, por ejemplo: modelos 3D, texturas, materiales, música y efectos de sonido, etc (ibid).

4.3 Riesgos en las redes sociales y ataques informáticos

En la presente investigación se abordan temas relativos a los riesgos en las redes sociales, como sexting y grooming, los ataques informáticos, hoax, phishing y spoofing. Fueron seleccionados por las consecuencias sociales extremas (suicidios) y por ser las más comunes. A continuación, se enuncian cada uno de los conceptos de acuerdo con las posturas teóricas de algunos autores.

4.3.1 Riesgos en las redes sociales

Sexting, es un concepto que surge a partir de las TIC y las redes sociales, Davidson (2015) afirma: “sexting es el intercambio de mensajes sexualmente explícitos a través de medios digitales” (p.1). Dichos mensaje o imágenes pueden ser difundidas en Internet y las personas pueden quedar en riesgo de pérdida de privacidad y/o violación a la intimidad o ser víctimas de extorsión.

Por otra parte, existe otro riesgo en las redes sociales, el Grooming, concepto que genera diversas posturas acerca de su definición, la UNICEF (2014) sostiene: “se llama grooming a la

acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de Internet. Siempre es un adulto quien ejerce el grooming.” (p.1). Dicha confianza usualmente es usada con intenciones negativas y puede desencadenar en abuso sexual.

4.3.2 Ataques informáticos



Ilustración 2: Ataques informáticos incluidos en el mundo virtual

A la par con la masificación de las TIC y la revolución del Internet, en la actualidad existen muchos tipos de ataques que amenazan la información en alguna de sus características principales, confidencialidad, integridad y disponibilidad, afectando a las personas ya sean naturales o jurídicas y dichos ataques pueden generar consecuencias económicas y/o vulnerarse su privacidad. En el recurso educativo se enuncian los siguientes conceptos:

Hoax, consisten en enviar mensajes al usuario pidiéndole que actúe de una manera particular, el mensaje induce una recompensa o regalo. En la plataforma de mensajería WhatsApp los estafadores intentan engañar a los usuarios (Shambhu, 2016). Los mensajes más conocidos se refieren a ayudas humanitarias o algún personaje de reconocimiento mundial repartiendo su

fortuna, etc. Por otra parte, pretenden recolectar información de los usuarios para nutrir bases de datos que posteriormente pueden ser vendidas o utilizadas con otro fin.

Uno de los ataques informáticos más peligrosos es el *phishing*. Es un término inglés que hace referencia a la pesca y aunque tiene varios tipos, se utiliza principalmente para la obtención fraudulenta de las claves de acceso de la banca en línea del usuario (Pere y Oliver, 2015). Los atacantes utilizan diferentes medios como el correo electrónico para obtener información de cuentas bancarias con un sitio web idéntico al original, o para vender productos que no cumplen con lo publicitado o para ofrecer servicios que simulan como gratuitos y no lo son.

Otro ataque informático es el *spoofing*, se refiere a la suplantación de identidad y puede ser de varios tipos. Pere y Oliver (2015) lo enuncian como:

Conjuntos de técnicas de suplantación de identidad. El atacante crea un contexto falso para engañar a la víctima con el objetivo de que facilite información confidencial como nombres de usuario y contraseñas. Los ataques de spoofing (contexto falso) son posibles tanto en el ciberespacio -creando una web falsa- como en el mundo físico, consiguiendo claves y contraseñas mediante llamadas telefónicas a empresas y particulares. (p.240)

En otras palabras, el spoofing es un tipo de ataque que hace creer a la víctima que se está comunicando con un equipo de confianza o autorizado y el atacante suplanta dicho dispositivo para adquirir información.

4.4 Normatividad Legal

Es importante destacar algunos artículos de la Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones (2016), que se refieren a Seguridad Informática:

LEY 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos y se preservan

integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas

electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con penas más graves.

5. ESTADO DEL ARTE

A continuación, se bosquejan algunos documentos científicos relacionados con las tendencias en la educación a nivel mundial, el modelo ARCS del profesor John Keller, y los mundos virtuales como estrategia innovadora que los docentes y/o investigadores están implementando en su ejercicio profesional a la par con los avances tecnológicos, la globalización, las herramientas web 2.0, 3.0 y 4.0, etc., desde los puntos de vista de apropiación, uso y aplicación en diferentes áreas del conocimiento, y por último, estudios realizados acerca de los riesgos en las redes sociales y ataques informáticos.

A continuación, se presenta una imagen (ilustración 2) de los resultados del Horizon Report 2016 (New Media Consortium [NMC], 2016) que enmarca en un estudio las principales tendencias a nivel mundial en la educación superior. Dicho reporte concreta los temas, desafíos y tendencias a corto mediano y largo plazo de acuerdo a la investigación correspondiente al 2016.

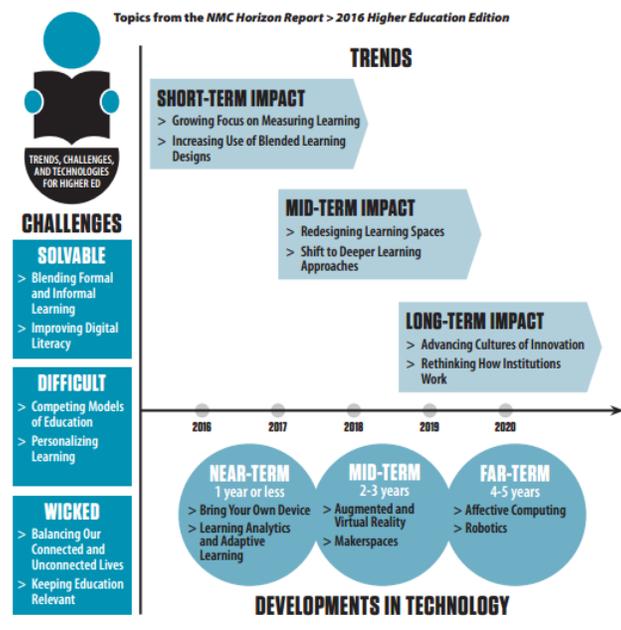


Ilustración 3: Horizon Report 2016 (New Media Consortium [NMC], 2016)

Se observa que las tendencias están íntimamente ligadas con las herramientas TIC y algunos nuevos conceptos como “Bring Your Own Device” (trae tu propio dispositivo), el Internet de las cosas, realidad aumentada y realidad virtual, este último relacionado con la presente investigación, la masificación y desarrollo de dicho concepto se espera a mediano plazo, es decir en los próximos 2 a 3 años (Ibid).

En lo que respecta a estudios relativos a la percepción de los estudiantes en relación con su motivación en el aprendizaje, se presentan algunos resultados de dichas investigaciones. Tapia (2005) concluye:

Merece la pena destacar por su efecto positivo sobre la motivación el hecho de que el profesor muestre la utilidad de aprender el contenido, la organización y claridad expositivas y la posibilidad de revisar la nota en privado para aprender. El uso generalizado de las pautas mencionadas favorecerá, pues, probablemente, la motivación por aprender de la mayoría de los alumnos. (p.21)

Se resalta del estudio anterior la equivalencia que existe entre los aspectos mencionados como la curiosidad, definir las metas u objetivos, la relevancia de los contenidos y los efectos positivos que generan la satisfacción y los principios del modelo ARCS: Atención, relevancia, confianza y satisfacción, respectivamente.

Acerca de la mediación tecnológica incorporada en la presente investigación, los mundos virtuales, hay que mencionar que no es una tecnología nueva, sin embargo, su uso en la educación se encuentra en etapa experimental. Así, “los mundos virtuales constituyen un escenario en el que todavía los docentes actúan como pioneros, experimentando metodologías de aprendizaje e investigando las potencialidades de estos espacios para complementar o enriquecer la enseñanza online o incluso la presencial” (García y González, 2011). Sin embargo, para poder aprovechar su potencial, se hace necesario contar con algunos recursos mínimos para poder implementar dicha tecnología como, por ejemplo, un ancho de banda adecuado, si se requiere

conexión a Internet, equipos de escritorio o dispositivos móviles para cada estudiante y con prestaciones adecuadas para la ejecución correcta del mundo virtual.

Por otra parte, en estudios realizados por diferentes autores que han utilizado mundos virtuales como herramienta pedagógica, han observado ventajas en el proceso de aprendizaje, por ejemplo:

Se ha producido un incremento de la motivación del estudiante percibido a través de las propias observaciones de los alumnos que han comentado positivamente, apuntándola como un recurso motivador, un recurso que rompe la monotonía del online, un acercamiento al profesor, un acercamiento a los compañeros de curso (García y Gonzalez, 2011).

Dichas ventajas están relacionadas con la motivación de los estudiantes en el logro del aprendizaje mediado por TIC, en donde se ha cambiado el esquema del aprendizaje tradicional. Por otra parte, es fundamental el evidenciar la transformación del conocimiento en los estudiantes por medio de la información adquirida por medio del recurso digital.

Lo anterior evidencia la eficacia de los mundos virtuales con objetivos pedagógicos en lo relativo con la motivación del estudiante, porque presenta de forma diferente los contenidos y existe interacción entre los participantes.

Sin embargo, los mundos virtuales presentan algunas limitaciones técnicas. Según (Márquez, 2010) no son accesibles a todo el mundo por razones presupuestales, geográficas y técnicas, como ancho de banda, hardware o discapacidad. Más interesante, son los aspectos derivados de los errores que continuamente se producen en la plataforma, simbolizados por la experiencia del “lag” (retraso).

A pesar de las dificultades anteriormente mencionadas, en la actualidad y con las tendencias en el sector educativo el uso de los mundos virtuales son una herramienta pedagógica viable en un entorno que brinda las condiciones adecuadas para su implementación. Al respecto, Kelton

(2008) refiere que es innegable, en la era del Internet y la globalización, el movimiento hacia el mundo virtual como una enseñanza viable en un entorno de aprendizaje que parece imparable.

Los resultados de algunos estudios lo confirman. Así, se ha producido un incremento de la motivación del estudiante percibido a través de las propias observaciones de los alumnos que han comentado positivamente, apuntándola como un recurso motivador, en conjunto, la experiencia educativa en el mundo virtual Second Life ha sido gratificante y positiva para profesor y estudiantes, incentivando el interés por la materia y fomentando la comunicación (García y González, 2011). Las conclusiones del estudio anterior mencionan que el uso de los mundos virtuales en un proceso académico no solo incentiva la motivación en los estudiantes sino también en los docentes.

Sin embargo, a pesar de las bondades de los mundos virtuales educativos, deben ir de la mano de una estrategia pedagógica incorporada por el docente, el cual sirva de guía y refuerce los conceptos que sean necesarios en el ejercicio académico. Grings, Trein y Oliveira (2009) afirman:

Sin embargo, hay que recordar que la mera utilización de los mundos virtuales 3D ya que son una novedad, no significa necesariamente la innovación en el contexto educativo. Para que esto suceda se necesita que los profesores / investigadores que se apropien de esta tecnología para entenderlo en el contexto de su naturaleza específica, la cual exige nuevas metodologías, prácticas de enseñanza y los procesos estén en sintonía con el potencial que ofrecen los mundos virtuales 3D. (p.31)

Como consecuencia, el uso de mundos virtuales en la educación implica innovar en estrategias didácticas, metodologías de evaluación y en las actividades de refuerzo, conservando el diseño motivacional, mencionado en el capítulo anterior. A continuación, se enuncia otro argumento similar, esta vez relacionado con los videojuegos en el aula. Así, claramente, los videojuegos, por sí mismos, no generan una mejora en los procesos cognitivos ni en la calidad

educativa, sino que esto depende sustancialmente de la planificación pedagógica que se lleve a cabo (Del Moral, Martínez, Tosina y Esnaola, 2012). Por lo tanto, debe existir un modelo, teoría o diseño pedagógico como base en los videojuegos educativos, además de la intencionalidad pedagógica.

En cuanto a las investigaciones relativas a los riesgos en las redes sociales y los ataques informáticos, se indagan algunos estudios al respecto. Pero es importante mencionar que los conceptos anteriores están enmarcados dentro de la seguridad informática, la cual se define como: “el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos” (Voutssas, 2010, p.131). Como consecuencia, todas las personas deben tener un mínimo de conocimientos del concepto anterior, algunas de sus características principales y de las políticas de protección de la información.

En el caso de los riesgos de las redes sociales, se observa en algunos estudios la percepción que tienen los estudiantes acerca del tema, por ejemplo, Lenhart (2009) concluye:

Las actitudes de los adolescentes hacia el sexting varían ampliamente, desde aquellos que no creen que es un tema importante, hasta algunos que piensan que es apropiado y para otros potencialmente dañino o ilegal. En un extremo del espectro están los adolescentes que ven al sexting como una alternativa más segura a la actividad sexual de la vida real. (p.13)

Lo anterior significa que los estudiantes no conocen el riesgo real, ni la forma de actuar en caso de ser víctima de sexting o grooming, ni las consecuencias a las que se exponen, que en el peor de los casos ha llevado a suicidios en adolescentes.

Por otra parte, es importante conocer los ataques informáticos más comunes, Voutssas (2010) afirma: “hoy en día la información es un activo muy valioso para casi todas las organizaciones; para algunas de ellas es su activo más valioso y por ello se invierten considerables recursos en crearla, administrarla, mantenerla, distribuirla, etcétera” (p.3). En pocas palabras, los ataques informáticos tienen como consecuencia pérdida de recursos económicos o afectación de la intimidad o privacidad.

6. MATERIAL EDUCATIVO

El material educativo es un mundo virtual desarrollado por la necesidad existente en la Universidad de Cundinamarca de utilizar herramientas TIC innovadoras en el aprendizaje de riesgos en las redes sociales y ataques informáticos. El diseño instruccional implementado en el recurso educativo es el modelo ARCS del profesor John Keller (2009). Fue implementado en un grupo de 16 estudiantes de Ingeniería de Sistemas en una sala de cómputo de la Universidad de manera presencial.

6.1 Descripción del material educativo

El material educativo fue diseñado e implementado en su totalidad por el investigador y se utilizan algunos elementos libres de la tienda de Unity (Ibid), por otra parte, se enlazan videos de campañas contra el sexting, el grooming y algunos de la plataforma TED (Technology, Entertainment, Design), en la siguiente tabla se listan las referencias de los recursos usados (Ver referencias en Tabla 1).

En la fase de diseño se realizó un Story Board (Anexo 2), se plasmó la idea inicial, con los diferentes escenarios del tour virtual, los elementos multimedia a incorporar al igual que los conceptos a incluir. Posteriormente, se desarrolló el material educativo, un tour virtual por una isla a la cual el usuario llega por medio de un helicóptero (Ilustración 4) y se encuentra con 2 preguntas detonadoras que lo cuestionan acerca de los conocimientos que posee acerca de los riesgos en las redes sociales y de tres ataques informáticos (Hoax, Phishing y Spoofing). Cruz (2010) define la pregunta detonadora como: “un pensamiento, un acontecimiento, cualquier hecho o material en medio y en cualquier punto del camino, del cual brotará un sin fin de

conocimientos y aprendizajes” (p. 56), por lo cual, es el punto de partida del tour virtual, indagando a los estudiantes sobre su conocimiento de la temática en estudio.



Ilustración 4: Punto de partida tour virtual

El recorrido inicia en una edificación llamada el Palacio de la Seguridad, en la entrada se encuentra un modelo 3D de un robot el cual resguarda el palacio (ilustración 5).

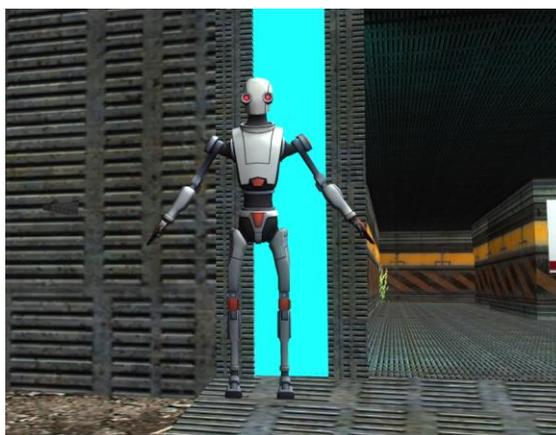


Ilustración 5: Ingreso a los escenarios

Al ingresar, se encuentra con una sala en la cual se disponen algunos monitores con el objetivo del material educativo, instrucciones de uso y un mapa del sitio en el que se ilustran los tres escenarios en su interior: el primero, acerca de los riesgos en las redes sociales, el segundo,

relativo a ataques informáticos y el último es una sala con videos de la plataforma TED (ilustración 6 y 7).

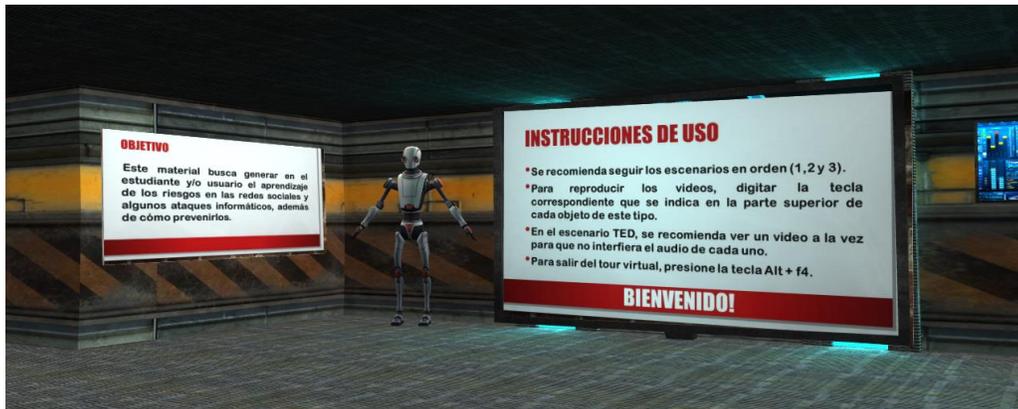


Ilustración 6: Objetivos, instrucciones de uso



Ilustración 7: Mapa del sitio

Posteriormente, el estudiante transita por un corredor en el que encuentra los tres escenarios anteriormente mencionados y puede decidir cuál tomar primero. En el primer escenario relativo a los riesgos en las redes sociales, se disponen videos que ilustran casos de Sexting y Grooming y dos presentaciones en las cuales se conceptualizan los riesgos, además, se proponen algunas recomendaciones para evitarlos (ilustración 8).



Ilustración 8: Escenario de Riesgos en las Redes Sociales

En el siguiente escenario referente a los ataques informáticos, principalmente: hoax, phishing y spoofing. Dichos conceptos se ilustran mediante posters y presentaciones con la definición de cada uno, los tipos, características y cómo prevenirlos (ilustración 9).



Ilustración 9: Escenario de Ataques Informáticos

En el último escenario, se encuentran 4 monitores, (ilustración 10 y 11) en los cuales el estudiante puede elegir entre igual número de conferencias de la plataforma TED, relativas a conceptos de seguridad informática. En las siguientes imágenes se puede observar la temática de dichos videos y los expositores:



Ilustración 10: Conferencias TED



Ilustración 11: Escenario TED

6.2 Descripción de la estrategia Pedagógica

En primer lugar, se desarrollo un pilotaje con un grupo de estudiantes de tecnología informática de la Universidad Minuto de Dios, Centro Regional Zipaquirá, para diagnosticar y corregir los errores del tour virtual. Posteriormente, se realizó la implementación del material educativo en la

Universidad de Cundinamarca con 16 estudiantes de Octavo semestre de Ingeniería de Sistemas en un laboratorio de informática y fue desarrollado en su totalidad en una sesión presencial de 2 horas (ver ilustración 12).

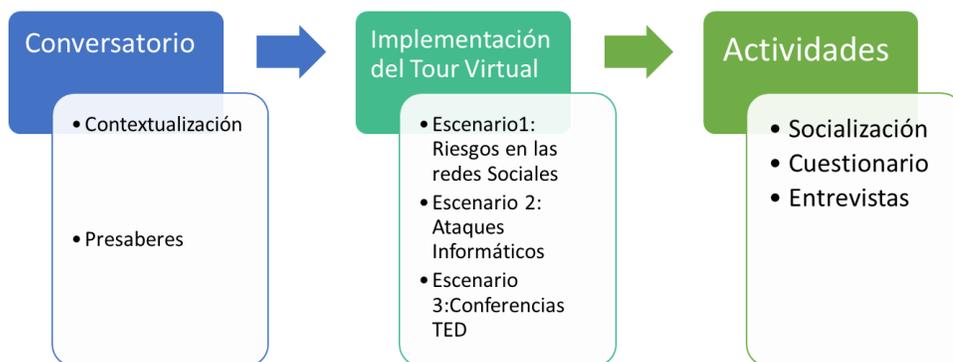


Ilustración 12: Fases de la Implementación del Material Educativo

Antes de iniciar con la implementación del material, el investigador realizó un conversatorio con los estudiantes con el propósito de compartir experiencias e identificar los conocimientos previos de los estudiantes relacionados con los riesgos en las redes sociales y ataques informáticos.

A continuación, se llevó a cabo la implementación del tour virtual en el que se encuentran tres escenarios que desarrollan la temática mediante la definición de los conceptos, principales características, consecuencias, ejemplificación y cómo prevenirlos o actuar en caso de ocurrencia. Por otra parte, los recursos utilizados en el mundo virtual fueron seleccionados y diseñados en función de cada uno de los principios del modelo ARCS.

Finalmente, se desarrollaron diferentes actividades: la socialización de la actividad, un cuestionario y entrevistas, que permitieron verificar los resultados y el logro de los objetivos acerca de los conocimientos de los estudiantes relativos a los riesgos en las Redes Sociales y ataques informáticos. La socialización permitió al investigador aclarar algunas dudas relativas a conceptos técnicos especialmente en los tipos de ataques informáticos y su funcionamiento.

6.3 Análisis del material educativo digital

Para el análisis del material educativo se siguieron los parámetros que constan en el formato de (Gregori., Majós., Onrubia. y Aguado, 2008). Por tanto, su desarrollo y evaluación fueron realizadas por el investigador y los resultados están consignados en el Anexo 1.

6.3.1 Dimensiones Evaluadas

a. Identificación y características generales del material.

En este acápite se identificaron los siguientes objetivos del Recurso Educativo Digital:

- Identificar riesgos en las redes sociales (grooming y sexting)
- Ilustrar los ataques informáticos: Hoax, Sexting y Grooming.
- Reconocer algunas buenas prácticas para minimizar los riesgos en las redes sociales y los ataques informáticos.

b. Accesibilidad y facilidades de uso:

Para el recorrido del mundo virtual no es necesario el uso de Internet y los equipos deben tener un Sistema operativo Windows 7 o superior, en caso de tener un sistema operativo diferente (MAC o Linux), el docente puede suministrar el material correspondiente. El tour virtual inicia mediante un archivo ejecutable y posteriormente el usuario puede seleccionar la resolución y las funciones del teclado para el desplazamiento (ilustración 13).

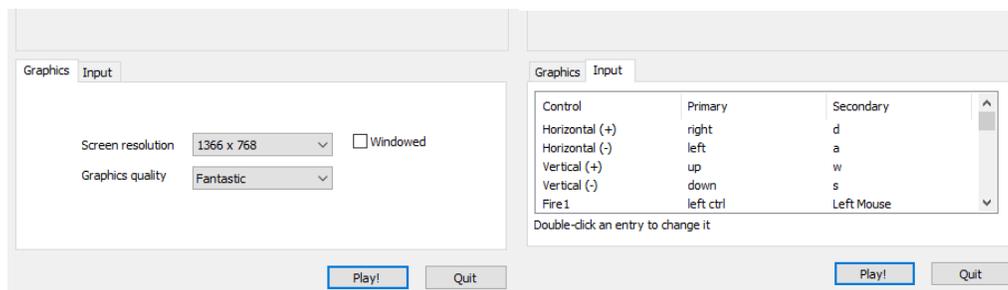


Ilustración 13: Opciones de configuración gráfica y controles

c. Características multimedia del material.

El material educativo presenta texto oral y escrito con imágenes en movimiento y sonidos. El mundo virtual incluye 4 videos de la plataforma TED, videos de casos de riesgos en las redes sociales, presentaciones y posters con los temas mencionados. En la siguiente tabla se presentan las referencias de los recursos utilizados que no son de autoría del investigador.

Tabla 1
Tabla de referencias de recursos utilizados

NOMBRE	CATEGORIA	AUTOR	UBICACIÓN	DESCRIPCIÓN
DESTROYED CITY	Modelo 3D Models/Environments /Sci-Fi	Profi Developers	https://www.assetstor.e.unity3d.com/en/#!/content/6459	Modelo 3d isla
SCI-FI LEVEL	Modelo 3D Models/Environments /Sci-Fi	Mixed Dimensions	https://www.assetstor.e.unity3d.com/en/#!/content/9595	Modelo 3d escenario
ORGANODRON CITY	Modelo 3D Models/Environments /Sci-Fi	Herminio Nieves	https://www.assetstor.e.unity3d.com/en/#!/content/9595	Modelo 3d fachada palacio
HH-65C DAUPHIN	3D Models/Vehicles/Air	AEgis Technologies	https://www.assetstor.e.unity3d.com/en/#!/content/8128	Modelo 3d Helicóptero
SPACE ROBOT KYLE	3D Models/Characters/Ro bots	Unity Technologies	https://www.assetstor.e.unity3d.com/en/#!/content/4696	Modelo 3d Robot
CAMPAÑA CONTRA EL GROOMING	Video	PDI - Policía de Investigacione s de Chile	https://www.facebook.com/video.php?v=980243862007429	Video de campaña contra el Grooming http://www.pdichile.cl/ https://www.facebook.com/hashtag/todoscontraelgrooming?source=embed

CAMPAÑA CONTRA EL SEXTING	Video	Protección online.com	https://www.youtube.com/user/protecciononline	Video de campaña contra el Sexting
WHAT WILL A FUTURE WITHOUT SECRETS LOOK LIKE?	Video TED	Alessandro Acquisti	https://www.ted.com/talks/alessandro_acquisti_why_privacy_matters	Video acerca de la importancia de la Privacidad
THINK YOUR EMAIL'S PRIVATE? THINK AGAIN	Video TED	Andy Yen	https://www.ted.com/talks/andy_yen_think_your_email_s_private_think_again	Video acerca de seguridad en e-mail
EVERYDAY CYBERCRIME AND WHAT YOU CAN DO ABOUT IT	Video TED	James Lyne	https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it	Video acerca del Ciberdelito
WHAT'S WRONG WITH YOUR PASSWORD?	Video TED	Lorrie Faith Cranor	https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_password	Video acerca de seguridad en passwords.
PIRATA	Imagen Libre	J.J.	https://ca.wikipedia.org/wiki/Pirateria_mar%C3%ADtima	Imagen de Pirata
POWTOON	Herramienta	-	http://www.powtoon.com/home/g/es/	Las presentaciones fueron realizadas con esta herramienta.

d. Presentación, organización y secuenciación de los contenidos.

El material educativo tiene una secuencia global de aporte de información, explicación y ejemplificación. Tiene un ritmo adecuado en la presentación de los contenidos, estos últimos se

presentan en cuatro escenarios, el primero, se dan las instrucciones iniciales de uso, los objetivos pedagógicos y el mapa del sitio. Y en los demás, se disponen unas presentaciones con la teoría de cada uno de los conceptos, unas imágenes con recomendaciones para evitar los riesgos en las redes sociales y los ataques informáticos y unos videos con ejemplos de cada tema. Por otra parte, en la sala TED fueron seleccionados e incorporados por parte del investigador cuatro temáticas relativas a seguridad informática. El usuario puede recorrer de manera secuencial o aleatoria los escenarios.

e. Tratamiento instruccional de los contenidos.

El material presenta frecuentemente elementos de refuerzo en la comprensión de contenidos mediante ejemplificaciones con el uso de videos. No incluye actividades de autoevaluación, por la naturaleza del material y porque existen algunos conceptos técnicos en el tour virtual que son desconocidos para los estudiantes, como por ejemplo ACL (Listas de Control de Acceso), IPsec (Protocolo de seguridad), o los tipos de Spoofing, que deben ser socializados por el docente al final del tour virtual. Al finalizar el recorrido, se realiza una socialización para identificar las dudas de los estudiantes y consolidar los conceptos de los temas expuestos en el material de aprendizaje.

El material globalmente es adecuado para el uso de procesos formativos presenciales y semi-presenciales y en función de la perspectiva de utilización posibilita al usuario seleccionar los controles de teclado para el desplazamiento y la resolución gráfica del tour virtual. El tour virtual se instaló en equipos recientemente adquiridos por la Universidad, en la sala de sistemas No. 2 de la Universidad, la cual está aislada acústicamente del exterior y permite un ambiente propicio para la actividad.

7. METODOLOGÍA DE LA INVESTIGACIÓN

Este capítulo tiene como objetivo definir la ruta metodológica del proyecto de investigación, donde se especifican los objetivos, el contexto, tipo de investigación, la población, la muestra, los instrumentos de recolección de información, y el papel que el investigador tendrá en el proyecto. Por último, se definirán los resultados y hallazgos parciales, al implementar el instrumento de cuestionario a la muestra en estudio. Dicho análisis fue realizado con la herramienta QDA Miner, para realizar el análisis cualitativo de los datos obtenidos.

7.1 Pregunta de investigación

¿Cuáles son las características desde el punto de vista tecnológico y pedagógico que se observan en un mundo virtual de conceptos de seguridad informática en función de la percepción del estudiante como estrategia de aprendizaje?

7.2 Tipo de estudio

La investigación es de tipo cualitativa, descriptiva, porque pretende identificar los aspectos y elementos que debe tener un mundo virtual para el aprendizaje de conceptos de seguridad informática y utilizará un marco de estudio de caso, porque busca implementar nuevas herramientas pedagógicas para el aprendizaje de conceptos de seguridad informática y que tienen un impacto social, al respecto Stake (1998), afirma:

Estudiamos un caso cuando tiene un interés muy especial en sí mismo. Buscamos el detalle de la interacción con sus contextos. El estudio de casos es el estudio de la particularidad y de la complejidad de un caso singular, para llegar a comprender su actividad en circunstancias importantes. (p.11)

En coherencia con el presente estudio en el cual se examina la percepción del estudiante al utilizar este tipo de herramienta pedagógica en el aprendizaje de dichos conceptos. La unidad de análisis son los estudiantes de octavo semestre de Ingeniería de Sistemas de la Universidad de Cundinamarca, extensión Chía.

7.3 Contexto

El Proyecto Educativo Institucional (PEI) de la Universidad de Cundinamarca [UDEC] 2015, cita lo siguiente acerca de los inicios de la Universidad:

La Universidad de Cundinamarca como proyecto educativo, tuvo sus orígenes en la Ordenanza número 045 del 19 de diciembre de 1969 con la cual se creó el Instituto Técnico Universitario de Cundinamarca – ITUC -, como entidad responsable de ofrecer a la población egresada de la educación secundaria en el Departamento, programas de educación superior con duración entre los dos y los dos años y medio. (p.5)

Posteriormente, el Gobierno Nacional la reconoce como Universidad pública del orden departamental (...) UDEC (2015):

Los estudios con base en los cuales se hizo la solicitud para el reconocimiento como universidad, fueron elaborados en el año de 1990, presentados a las autoridades respectivas para su evaluación y sobre esta base, el 30 de diciembre de 1992 por resolución 19.530, el Ministerio de Educación Nacional hizo el reconocimiento como universidad. Desde entonces y hasta hoy, la Universidad de Cundinamarca ha estado avanzando responsable, constante y persistentemente, para consolidarse como la institución en la cual los habitantes de la provincia del Departamento encuentren las oportunidades de formación profesional que buscan, y para ser, al mismo tiempo, un centro de apoyo al desarrollo de los sectores económicos y sociales, aportándoles los resultados de su trabajo investigativo y los conocimientos de su cuerpo docente. (p.7)

La Universidad de Cundinamarca tiene presencia en 8 municipios del Departamento, Fusagasugá (que es la sede principal), dos seccionales, Girardot y Ubaté, cinco extensiones,

Soacha, Zipaquirá, Chocontá, Facatativá y Chía. En esta última se implementó el material educativo y cuenta con los programas de Ingeniería de Sistemas y Administración de empresas.

Es objetivo de la universidad formar a sus estudiantes como líderes, de manera integral y con grandes calidades humanas, como se plasma en su misión institucional (...) UDEC (2015) en la cual se afirma:

La Universidad de Cundinamarca es una entidad pública del orden departamental al servicio de la provincia, el departamento y la nación, responsable de la formación de profesionales líderes con altas calidades académicas, laborales y humanas. Está comprometida con la formación integral de un hombre en quien se desarrollen óptimamente, las diferentes dimensiones de su ser, y que actúe con base en el conocimiento de las condiciones culturales, sociales y ambientales de su entorno. La Universidad de Cundinamarca, para enriquecer la cultura universal y aportar al avance de las ciencias, desarrolla su gestión educativa a partir de la profundización en el conocimiento del entorno regional en que se encuentra ubicada, para elaborar saberes que permitan identificar y solucionar los problemas de orden social y natural propios y generar conocimientos útiles a la humanidad. (p.16)

7.4 Universo, población y muestra

El Universo de la presente investigación corresponde a los estudiantes de Ingeniería de Sistemas de la Universidad de Cundinamarca. La población son los estudiantes de la facultad mencionada de la extensión Chía, aproximadamente 300 alumnos y la muestra son 16 estudiantes de octavo semestre que cumplen con los siguientes criterios:

- a. Tienen conocimientos básicos acerca de programación de computadores.
- b. Grupo de estudiantes en un rango de edad entre los 19 a 35 años.
- c. Grupo compuesto por hombres y mujeres.
- d. Utilizan a diario las redes sociales e Internet.
- e. Pertenecen a los estratos socio-económicos 2 y 3.

Se garantiza el respeto a la integridad y dignidad de los participantes mediante la aplicación anónima de los instrumentos de medición y el correcto uso de la información obtenida y con la autorización previa mediante el formato correspondiente, donde se indica la naturaleza de la investigación y el uso de la información obtenida (Anexo 8).

7.5 Instrumentos

Se utilizarán los siguientes instrumentos para la recolección de información:

Diario de campo: este instrumento permite llevar los registros observacionales de los aspectos que se desean identificar en los estudiantes. García (2000) comenta: “El diario de campo sirve para proyectar las reacciones de la persona que investiga durante el ejercicio de su actividad. Sirve también para entender mejor la investigación, e incluso para analizar la realidad social” (p. 3). Se seleccionó porque facilita la labor de registro de los rasgos a observar en el momento de la implementación del Recurso Educativo Digital. Ver Anexo 3: Formato de Diario de campo.

Cuestionario: Este instrumento se utiliza al finalizar la sesión del tour virtual, Bernal (2006) lo define: “Se trata de un plan para recabar información de la unidad de análisis objeto de estudio y centro del problema de investigación” (p. 217). Busca registrar información acerca de los elementos que debe tener dicho material educativo para el aprendizaje de conceptos de Seguridad Informática y para cada una de las categorías de análisis de manera escrita. Ver Anexo 4: Cuestionario.

Entrevista: El tercer instrumento busca realizar la triangulación de los datos proporcionados para una mayor confiabilidad. Namakforoosh (2000) afirma: “la entrevista personal tiene la ventaja de que el entrevistador puede dirigir el comportamiento del entrevistado” (p. 140), por lo anterior, con este elemento es posible verificar los hallazgos mediante una observación directa y realizar preguntas adicionales según se requiera. Ver Anexo 5: Entrevista.

7.6 Papel del investigador

El investigador desempeña un rol de observador y no tendrá injerencia en los datos obtenidos. La metodología anterior, establece los pilares del proyecto de investigación, y la ruta a seguir en su desarrollo.

8. RESULTADOS

La presente investigación busca identificar la percepción del estudiante en función de las características pedagógicas y tecnológicas de un mundo virtual en el aprendizaje de conceptos de seguridad informática. Los datos suministrados por los instrumentos (Diario de campo, cuestionarios y entrevistas), son el objeto de estudio del presente capítulo. Las siguientes imágenes corresponden a la sesión de implementación del material educativo y posteriormente se describen las diferentes categorías en estudio, en concordancia con el diseño instruccional, el modelo ARCS. Las siguientes fotografías corresponden al momento de la implementación del material (Ilustración 14).



Ilustración 14: Fotos de Implementación del material educativo.

8.1 Categorías de análisis

De acuerdo con el objetivo de la investigación, se concretaron 2 categorías a priori: percepción y confianza. Después, al realizar el análisis de los datos surgieron las categorías emergentes: recursos, características técnicas, contenidos y dificultades.

Finalmente, las categorías recursos y características técnicas se fusionaron en la categoría atención. Por otra parte, las categorías emergentes, contenidos y dificultades se agruparon en la categoría relevancia. De lo anterior, resultan las categorías de análisis: percepción, confianza, atención y relevancia, en paralelo con los principios del modelo ARCS, como se observa en el siguiente gráfico (Ilustración 15).



Ilustración 15: Fusión de Categorías de Análisis

Percepción: En esta categoría se analizan las sensaciones, opiniones, experiencias, motivación y conceptos de los participantes al interactuar con el Material Educativo Digital. En relación con la experiencia del usuario, el estudiante debe disfrutar del propio aprendizaje mediante el uso de los recursos educativos procurando que este les ofrezca recompensas positivas (Rué, 2009). Lo anterior se logra, apropiando las TIC como herramienta creadora o mediadora entre el aprendizaje y los recursos.

Confianza: Se refiere al análisis de los logros del mundo virtual como herramienta pedagógica para brindar conocimientos sobre los riesgos de las redes sociales y los ataques informáticos

adquiridos al interactuar con el Material Educativo Digital. El estudiante adquiere el conocimiento de la temática por el recorrido en el tour virtual como también influye el entorno en que se desarrolla. Así, el material sirve de ayuda en el momento de impartir un conocimiento y cómo se le incluya en la propuesta pedagógica implicará el lugar de entorno o la colaboración para el usuario (Litwin, 2005). Por lo anterior, el material servirá como herramienta educativa y el investigador tiene un papel de observador durante la implementación del tour virtual.

Atención: En esta categoría se indagan los diferentes recursos utilizados en el material educativo como videos, conferencias, animaciones, lecturas, poster, etc., en relación con la percepción del estudiante acerca de las características técnicas de dichos elementos, además de analizar si despierta en ellos el interés, la curiosidad o si resultan atractivos y de fácil comprensión. Alarcón y Navarro (2014) afirman: “la idea no es sólo captar la atención del estudiante, sino conservarla, de ahí la importancia de elegir los estímulos adecuados o las estrategias motivacionales que sirven especialmente para mantener la atención y el interés” (p.43). Las estrategias fueron implementadas en los recursos del mundo virtual y son objeto de análisis de la presente categoría.

Relevancia: Hace referencia a la pertinencia de los contenidos del Material Educativo Digital, si están alineados con sus necesidades, además de identificar los aprendizajes acerca de la temática. Méndez-Ibáñez., Martí-Parreño, Queiro-Ameijeiras, y Giménez-Fita, (2015) mencionan: “El factor relevancia está relacionado con la asociación percibida por el estudiante entre los conocimientos previos y la nueva información aportada por el videojuego educativo, así como la relevancia de estos nuevos conocimientos aportados a los intereses del estudiante”. Lo anterior, refleja la voluntad de aprender por parte del estudiante al percibir un nuevo conocimiento, partiendo de unos conocimientos previos. En paralelo, los participantes tienen

conocimientos previos de informática, hacen uso de las redes sociales, navegan de manera cotidiana en Internet y se observa la voluntad de aprendizaje en concordancia con la temática.

8.2 Red Semántica

La relación entre las categorías de análisis, percepción, atención, confianza y relevancia se muestra en el siguiente gráfico de redes semánticas (Ilustración 16).



Ilustración 16: Red Semántica

La categoría percepción se centra en las diferentes experiencias de los estudiantes en el tour virtual y está asociada con las demás categorías de análisis, confianza, atención y relevancia. La relación entre percepción y confianza son los logros del tour virtual como herramienta pedagógica. Por otra parte, el enlace percepción – atención, corresponde a las sensaciones de los estudiantes acerca de los recursos o elementos implementados en el mundo virtual. Por último, la asociación entre percepción – relevancia, son las diversas opiniones acerca de los aportes de la temática y las dificultades de uso.

8.3 Resultados por categoría de análisis

El resultado específico desde el punto de vista pedagógico se encuentra inmerso dentro de los hallazgos para cada una de las categorías del modelo instruccional seguido de conformidad con los datos suministrados por los tres instrumentos de la investigación: el cuestionario, las entrevistas y el diario de campo.

El cuestionario, fue aplicado a 16 estudiantes de octavo semestre de Ingeniería de Sistemas de la Universidad de Cundinamarca. La entrevista fue aplicada a 4 estudiantes del grupo en mención y el diario de campo contiene las anotaciones y comentarios observados por el investigador durante el desarrollo del presente estudio y la aplicación del material de acuerdo con el formato respectivo (Ver anexo 3).

Percepción: En los siguientes gráficos se observan los resultados para la categoría mencionada de conformidad con las respuestas al cuestionario resuelto por los estudiantes:

En cuanto a la temática abordada, el 44% de los alumnos consideran que el mundo virtual incluye una temática importante porque abarca temas actuales relativos a la seguridad informática no contenidos en el programa de Ingeniería de Sistemas. También opinan que los fenómenos de los riesgos en las redes sociales, la vulnerabilidad de los datos personales y los ataques informáticos pueden afectar a cualquier usuario de Internet. Por otra parte, el 32% consideran interesante la temática del mundo virtual, porque es una línea de profundización de la carrera de Ingeniería de Sistemas no obstante a que la información es básica pero entendible. A su vez, el 24% restante opinan que los temas son: apropiados (6%), válidos y pertinentes (6%), conferencias interesantes (6%) y el tour virtual excelente (6%) (Ilustración 17).



Ilustración 17: Gráfica de la categoría Percepción

En lo que se refiere a la percepción de los estudiantes acerca de los aspectos a mejorar en el tour virtual, el 38% de los alumnos considera que se deben incorporar actividades de juego con preguntas acerca de los conceptos aprendidos o relacionando términos con enunciados, ganando puntos por cada acierto. Además, el 13% recomienda implementar otro avatar con un rol de guía con el cual interactuar y que brinde recomendaciones e incentivos a lo largo del recorrido. Por otra parte, el 13% exhorta a mejorar los controles en el mundo virtual principalmente en los videos de las conferencias para facilitar el pausar/reproducir. El porcentaje restante opina que se deben incluir la temática acerca de hacking ético, tipos de virus, etc. (12%), programas que brinden protección (6%), que no hay ningún aspecto a corregir (6%), ninguna mejora (6%) y ¿qué hacer? en caso que se materialice alguno de los riesgos (6%) (Ilustración 18).



Ilustración 18: Gráfica de la categoría Percepción

Los hallazgos anteriormente mencionados, se reafirman con la percepción de los estudiantes acerca del tour virtual en las entrevistas realizadas. Los comentarios al respecto se consignan a continuación:

C1: “El juego es pedagógico y los temas son interesantes”.

C2: “La pedagogía es divertida”.

C3: “Como estudiante de Ingeniería de Sistemas es necesario conocer los temas del tour para el día a día y en el desempeño laboral”.

C4: “Fue una actividad con la didáctica del juego muy divertida, con temas interesantes”.

C5: “Se deben integrar actividades de juego en la actividad”.

C6: “Me parecieron interesantes los temas de sexting, spoofing y cyberbulling”

C7: “Es muy importante conocer estos conceptos, por temas relacionados con la privacidad de la información e intimidad de cada persona”.

C8: “Muy interesantes los temas porque nosotros los jóvenes utilizamos mucho las redes sociales y desconocemos los peligros y el tipo de personas que quieren apoderarse de nuestra información personal”.

El investigador en su rol de observador realizó comentarios de cada una de las categorías de análisis de acuerdo con el instrumento diario de campo (DC) y cuyo formato se encuentra en el anexo 3. En relación con la categoría percepción, se registraron los siguientes:

DC1: “En general los estudiantes permanecieron motivados durante todo el recorrido del tour virtual y emitían comentarios de agrado acerca de la forma en que se presentó la temática, considerándola interesante, dinámica e interactiva”.

DC2: “La didáctica del tour virtual tiene semejanzas con un videojuego, estimula la curiosidad del estudiante por saber con qué elementos se encontrará en el material educativo y se percibe la voluntad de aprender por parte del alumno”.

DC3: “Algunos alumnos se mostraron interesados con el software de desarrollo Unity. Lo anterior, proporciona un valor agregado e incentiva al estudiante en la realización de objetos tridimensionales y materiales educativos de este tipo”.

Confianza: En esta categoría se identificaron hallazgos relacionados con los aspectos positivos percibidos por los estudiantes al recorrer el tour virtual y diferencias entre esta pedagogía y la tradicional.

Según los estudiantes, los principales logros que ofrece el implementar el mundo virtual como herramienta pedagógica son: el material educativo brinda nuevos conocimientos (57%), acerca de temas relacionados con privacidad, seguridad, redes sociales, tipos de amenazas, información personal, tráfico de pornografía de menores, falsificación en documentos, redes seguras, y la importancia que tiene la información y la privacidad. Además, lo consideran dinámico e interactivo (15%), porque se incluyen ejemplos de los riesgos y las conferencias realizadas por expertos. Por otra parte, expresan que el material educativo es ingenioso y creativo 14%, donde se exponen los contenidos de forma diferente dando uso de una nueva herramienta. Finalmente, es considerado como didáctico (7%) y brinda una información clara (7%). A continuación, se ilustran los resultados mencionados (Ilustración 19):

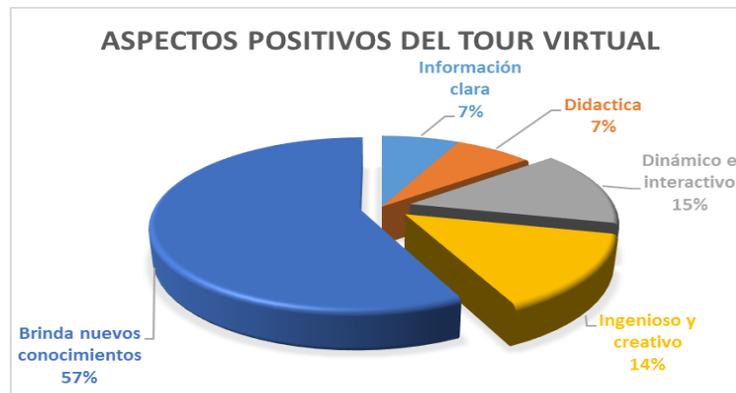


Ilustración 19: Gráfica de la categoría Confianza

Con respecto a las diferencias con la pedagogía tradicional los alumnos consideran el tour virtual como didáctico y dinámico (25%), el cual se caracteriza porque existe libertad en el recorrido y en la velocidad del aprendizaje, además que no se tiene contacto con el expositor. El 19% de los participantes lo define como atractivo con aspectos similares a los videojuegos. Motivador y didáctico (13%), innovador, interesante y divertido (13%), llamativo y menos monótono que las estrategias académicas tradicionales (12%). Por otra parte, lo perciben como innovador y divertido (6%), libertad en la escogencia del tema y recorrido (6%) y aprendizaje con interacción (6%). Dichas diferencias se exhiben a continuación (Ilustración 20).



Ilustración 20: Gráfica de la categoría Confianza

Los estudiantes consideran al tour virtual como didáctico, dinámico, divertido, motivador y como una herramienta pedagógica para el aprendizaje de los riesgos en las redes sociales. Los siguientes comentarios evidencian las diferencias de este tipo de pedagogías con la tradicional y los aprendizajes obtenidos referentes a los riesgos en las redes sociales.

C9: “Es una forma diferente de aprender, y los videos muestran con ejemplos reales”.

C10: “Los contenidos pueden verse las veces que se quiera, los gráficos son de gran calidad y la temática es muy interesante y se presentan de una manera diferente”.

C11: “Sexting, grooming, phishing y cyberbullying”.

C12: “Muy interesantes, conocía de algunos, pero no sabía cómo se llamaban”

C13: “Los temas tienen que ver con tecnología y los videos interesantes”.

Algunas de las observaciones realizadas por el investigador en relación con los logros en el aprendizaje de los estudiantes y del Recurso Educativo Digital son:

DC4: “Dado el interés que los estudiantes demuestran en relación con la temática y el implementar una herramienta de aprendizaje innovadora, se observa el logro en el aprendizaje de los conceptos”.

DC5: “Se observa un impacto mayor en la temática de los riesgos en las redes sociales sobre los conceptos de ataques informáticos, especialmente el sexting”.

Atención: Para esta categoría que está íntimamente ligada con los recursos utilizados en el tour virtual, se presentan los hallazgos en relación con las ventajas y los aspectos tecnológicos y pedagógicos a mejorar en el tour virtual. En lo que tiene que ver con las bondades de los elementos pedagógicos incluidos en el material educativo, los participantes consideran que los elementos incluidos en el tour virtual brindan conocimientos técnicos acerca de los riesgos, acerca de las vulnerabilidades y amenazas a la información personal (31%). También, valoran

que se puede utilizar en cualquier lugar y por diferentes tipos de usuarios y/o edades por la didáctica y la motivación, notable en el Recurso Educativo Digital (19%) y por los variados recursos utilizados como las presentaciones, posters o videos. Además, consideran que los recursos brindan conocimientos técnicos acerca de cómo prevenir los riesgos y los ataques informáticos (19%), la interactividad (13%), la importancia de protección de datos (12%) y la utilidad para todas las personas (6%), conocimiento que puede ser difundido a familiares y amigos. A continuación, se presenta un gráfico que ilustra los resultados al respecto (Ilustración 21).

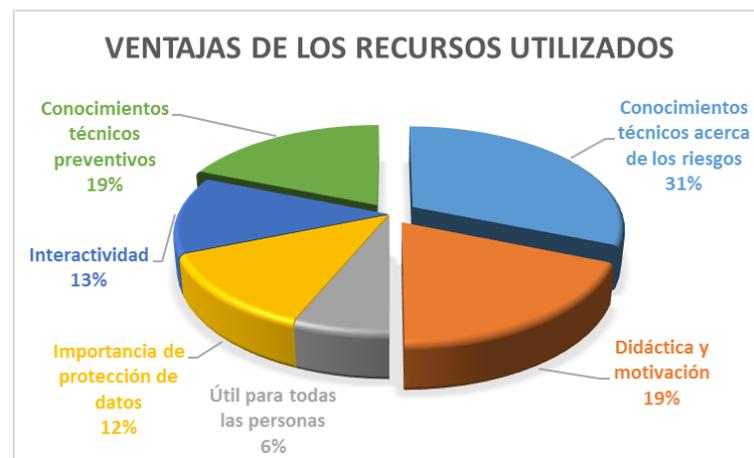


Ilustración 21: Gráfica de la categoría Atención

Por otra parte, los aspectos que se deben mejorar en el tour virtual según la percepción de los estudiantes se encuentran: incorporar controles en los videos (19%), dificultad que se hizo notoria al cambiar de escenario. Ampliar la temática (13%) e incluir conferencias de menor duración (13%) las cuales se desarrollaban en un promedio de 20 minutos. Además, eliminar los subtítulos de las conferencias TED (6%), en otras palabras, incluir videos en español para lograr mantener la atención en dicho recurso que en algunos casos generaban distracciones por esta causa (6%), al mismo tiempo, se debe mejorar la interactividad (6%) y tener en cuenta que los

conocimientos de las técnicas para realizar ataques informáticos pueden ser utilizadas con malas intenciones (6%) y el 31% consideran que no es necesario ninguna mejora (Ilustración 22).



Ilustración 22: Gráfica de la categoría Atención

Los recursos educativos presentes a lo largo de cada uno de los módulos del tour virtual, brindan algunos aspectos sobresalientes como la motivación, los conocimientos acerca de la prevención de los riesgos y la interactividad. Algunos comentarios de los estudiantes al respecto son los siguientes:

C14: “Se muestra la información de forma diferente e innovadora”.

C15: “El mundo virtual se puede recorrer de manera libre seleccionado el módulo que más considere conveniente y el profesor no dicta el tema directamente”.

C16: “Los gráficos son muy buenos, los videos muy interesantes, los escenarios modernos y la duración de la actividad es adecuada”.

C17: “Es diferente porque estamos acostumbrados a que los profesores usen los tableros o el videobeam, pero nunca he usado este tipo de software”.

C18: “A pesar de los subtítulos, los videos en inglés dificultan la comprensión de la totalidad de los conceptos”.

C19: “Incluir otros temas de seguridad informática, como informática forense, y como detectar los ataques informáticos y cómo enfrentarlos”.

Acerca de las estrategias y mejoras en relación con los recursos utilizados en el material educativo para conservar la motivación y la atención en los estudiantes, el investigador realizó los siguientes comentarios los cuales están consignados en el diario de campo (DC).

DC6: “Se observa que los estudiantes perciben como interesantes las temáticas de las conferencias de la plataforma TED, sin embargo, este recurso debe ser implementado con videos de máximo 10 minutos de duración, porque después de este tiempo los estudiantes se dispersan o distraen, principalmente por la presencia de la traducción al español por medio de subtítulos”.

DC7: “Las presentaciones elaboradas con algunas ilustraciones y variados elementos didácticos, facilitó el desarrollo de los contenidos, los cuales fueron considerados por los estudiantes como fáciles de entender”.

Relevancia: Los hallazgos encontrados para esta categoría tienen que ver con los conocimientos adquiridos por los estudiantes y la pertinencia de los contenidos. Entre los conceptos aprendidos en el recorrido del tour virtual se identificaron principalmente: Phishing (18%), Sexting (16%), Hoax (9%), Grooming (8%), Spoofing (7%), este último presentó algunas dificultades porque se mencionaron en el material varias clases de este tipo de ataque y se incluyeron conceptos técnicos como ACL (Listas de Control de Acceso) o el protocolo IPSec, los cuales fueron determinados al finalizar la actividad, y en otros conceptos (42%), incluidos los que citaron los expertos en las conferencias de la plataforma TED, entre los cuales se mencionan: virus, seguridad informática, privacidad, troyano, contraseñas, cifrado, hacking, ataques informáticos, riesgos en las redes sociales, riesgos en e-mail, manipulación de la información,

pornografía, cibersexo, información pública, malware, extorsión sexual, suplantación, cibercrimen, vulnerabilidad de la información (Ilustración 23).

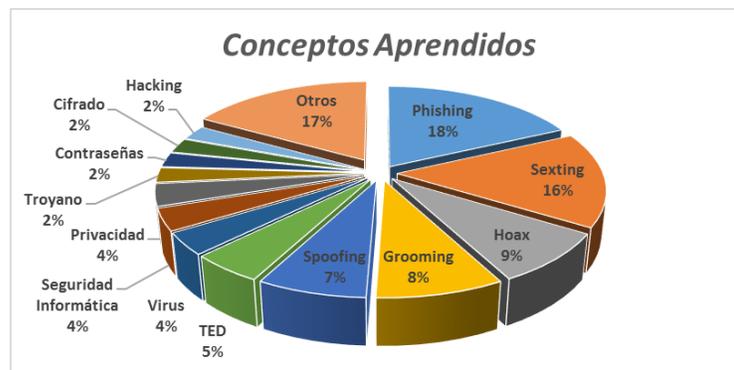


Ilustración 23: Gráfica de la categoría Relevancia

Al preguntar a los alumnos acerca de cuál es el aporte que les brinda el material educativo o en qué pueden aplicar los aprendizajes suministrados por el Recurso Educativo Digital consideran que los conocimientos adquiridos en el recorrido virtual les brinda herramientas acerca de algunas buenas prácticas de privacidad para minimizar los riesgos en las redes sociales (25%), además, les aporta en el ámbito laboral y personal (25%) y políticas de privacidad en la web (19%), por ejemplo, navegando en sitios seguros (13%), utilizando políticas de password (12%) e incluyendo módulos de seguridad en App (6%). La siguiente imagen refleja los hallazgos (Ilustración 24).

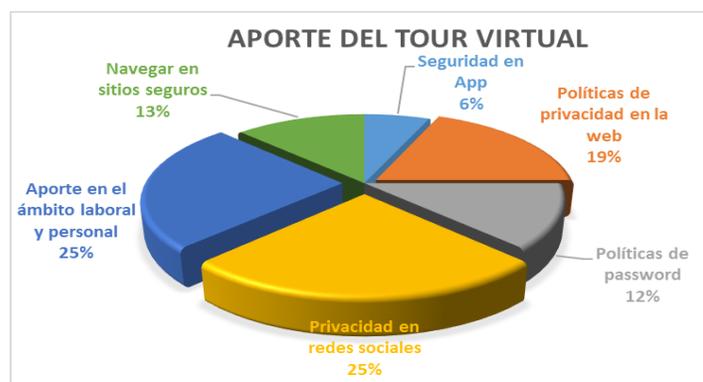


Ilustración 24: Gráfica de la categoría Relevancia

Para la categoría de relevancia se observó que los alumnos tuvieron como eje principal de aprendizaje los riesgos en las redes sociales. Entre los comentarios emitidos con relación a la presente categoría se encuentran los siguientes:

C20: “Muy interesantes los temas porque nosotros los jóvenes utilizamos mucho las redes sociales, y desconocemos los peligros y el tipo de personas que quieren apoderarse de nuestra información personal”.

C21: “Para proteger la información personal y aplicarlas en el trabajo”.

Algunos comentarios del investigador acerca de la anterior categoría son:

DC8: “Los casos de ejemplo de sexting y grooming tienen un impacto positivo en términos del aprendizaje y se observa que es uno de los mejores recursos a implementar en el tour virtual”.

DC: “Entre los inconvenientes de uso se observan la sensibilidad de movimiento, la falta de un menú para poder salir o configurar los controles en los videos y mejorar la interacción incorporando un personaje con un rol de guía”.

9. CONCLUSIONES

Los estudiantes tuvieron la oportunidad de recorrer e interactuar con los elementos y recursos del tour virtual de riesgos en las redes sociales y ataques informáticos y la presente investigación realizó el estudio correspondiente en función de su percepción de conformidad con las categorías de análisis del modelo ARCS del profesor John Keller (2009). Las conclusiones se resumen en las siguientes:

La tendencia de los estudiantes considera que el tour del mundo virtual tiene temas actuales relativos a seguridad informática y que su temática es importante, que los contenidos no han sido tratados en las cátedras del programa de Ingeniería de Sistemas de la Universidad de Cundinamarca y opinan que los fenómenos de los riesgos en las redes sociales, la vulnerabilidad de los datos personales y los ataques informáticos pueden afectar a cualquier usuario de Internet.

La percepción de los alumnos acerca de otros aspectos relacionados con la temática para mejorar el tour virtual, es gamificarlo, ya que recomiendan que se deben incorporar actividades de juego, implementar otro avatar con un rol de guía con el cual interactuar y brindar incentivos, premios o puntos a lo largo del recorrido.

También sugieren incorporar controles en los videos, ampliar la temática e incluir conferencias de menor duración, además, incluir videos en español para lograr mantener la atención en dicho recurso que en algunos casos generaban distracciones por esta causa.

Con respecto a las diferencias con la pedagogía tradicional los alumnos consideran al tour virtual como didáctico y dinámico y que lo caracteriza en la libertad en el recorrido, en la velocidad del aprendizaje y que no se tiene contacto con el expositor.

Entre las ventajas de los elementos pedagógicos incluidos en el mundo virtual exponen que brindan conocimientos técnicos acerca de los riesgos, vulnerabilidades y amenazas a la información personal. También, valoran que se puede utilizar en cualquier lugar y por diferentes tipos de usuarios y/o edades por la didáctica y la motivación.

Entre los conceptos aprendidos en el recorrido del tour virtual se identificaron, Phishing, Sexting, Hoax, Grooming y Spoofing, este último presentó algunas dificultades porque se mencionaron en el material varias clases de este tipo de ataque y se incluyeron conceptos técnicos como ACL (Listas de Control de Acceso) o el protocolo IPSec, los cuales fueron aclarados al finalizar la actividad. Así mismo, se identificó que debe existir un acompañamiento por parte del docente. Al respecto, el papel del profesor sigue siendo preponderante en el aula (aunque sea digital), pues es quien preside la clase dentro de las aulas virtuales.

Los aportes que les brinda el material educativo o en qué pueden aplicar los aprendizajes suministrados por el Recurso Educativo Digital consideran que los conocimientos adquiridos en el recorrido virtual les brinda herramientas acerca de algunas buenas prácticas de privacidad para minimizar los riesgos en las redes sociales, además, les aporta en el ámbito laboral y personal.

En definitiva, el principal logro que ofrece el mundo virtual como herramienta pedagógica es el brindar nuevos conocimientos acerca de conceptos relacionados con privacidad, seguridad, y tipos de amenazas a consecuencia del interés que los estudiantes demuestran en relación con la temática e implementar una herramienta de aprendizaje innovadora.

Adicionalmente, los elementos utilizados en el material como las presentaciones, los videos de casos de ejemplo y las conferencias son elementos didácticos que permiten el desarrollo de los contenidos, los cuales fueron considerados por los estudiantes como fáciles de entender. Para terminar, es importante mencionar los siguientes aspectos:

- a. Se reconoce un interés de los estudiantes por la temática abordada en el tour virtual, especialmente por los riesgos en las redes sociales.
- b. El uso de metaversos o de mundos virtuales en el aula de clase generan un valor agregado en la didáctica porque lo consideran innovador y divertido.
- c. Como resultado del proyecto se reconoce por parte de los estudiantes que el aprendizaje de los contenidos del Recurso Educativo Digital les brinda herramientas para proteger la información personal asociado con conceptos de privacidad e intimidad.
- d. Resulta muy importante realizar un acompañamiento por parte de los docentes, para aclarar las dudas de los estudiantes y los conceptos, por la naturaleza del material educativo.
- e. Es frecuente que los metaversos sean usados en asignaturas relativas al área de humanidades, artes o diseño, sin embargo, de acuerdo con los datos obtenidos se evidencia que un tour virtual contribuye en el aprendizaje de conceptos de seguridad informática y pueden ser usados en otras áreas del conocimiento.

10. PROSPECTIVA Y RECOMENDACIONES

El presente estudio utiliza un mundo virtual como herramienta pedagógica acorde con la necesidad de incorporar recursos educativos innovadores con la implementación eficiente de las TIC. Dado que los estudiantes usan de manera cotidiana las redes sociales y navegan en Internet, realizando compras en línea, transacciones bancarias, trabajos, etc., se determina que existen muchos riesgos que atentan contra la privacidad, la intimidad y en general con uno de los activos más importantes que puede tener toda persona, la información.

Todas las acciones que se tomen para generar conocimientos relativos al tema, resultan de gran ayuda para aprender a prevenir los riesgos en las redes sociales y los ataques informáticos para saber cómo actuar en caso de ser víctima de alguno de ellos, máxime en estudiantes de Ingeniería de Sistemas o carreras afines.

El material educativo incorpora recursos didácticos que pueden ser implementados también para estudiantes de secundaria y universitarios de todas las carreras con acompañamiento del docente para aclarar conceptos técnicos que maneja el material y para llevar a cabo las actividades y la coevaluación. La prospectiva de este material educativo tiene una cobertura general, que involucra a toda la sociedad por ser usuarios de las TIC, por lo cual se infiere que puede ser una herramienta eficaz e innovadora en el aprendizaje de la temática.

Dada la naturaleza del tour virtual, la interacción entre el estudiante, los recursos y los elementos del material educativo es evidente y se recomienda evolucionar la interactividad entre los estudiantes a nivel de videojuego, incorporando un software de mayor alcance e interdisciplinario, prospectiva que fue acogida en principio por la Universidad de La Sabana.

CRONOGRAMA

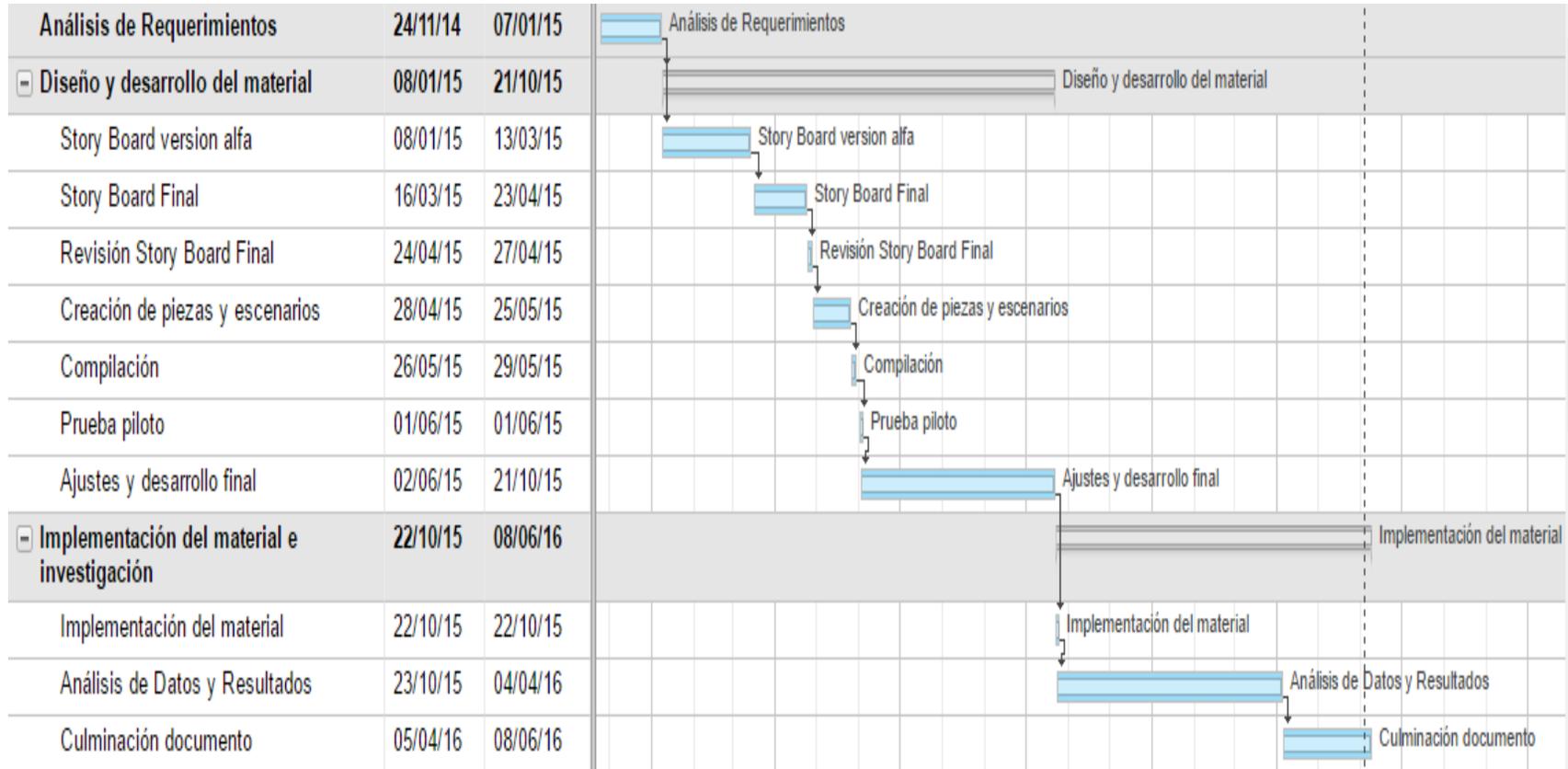


Ilustración 25: Cronograma

BIBLIOGRAFÍA

- Alarcón, L., y Navarro, J. (2014). Revisión del modelo atención, relevancia, confianza y satisfacción (ARCS). *Los Modelos Tecno-Educativos*, 41.
- Bernal, C. (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales*. Colombia: Pearson educación.
- Castronova, E. (2001). Virtual worlds: A first-hand account of market and society on the cyberian frontier. *CESifo Working Paper*. 618. 1-40
- Cruz Moreno, E. (2010). Cómo manejar la pregunta detonadora en un escenario virtual. *Revista Mexicana de Bachillerato a Distancia*, 2(4). 54-56
- Davidson J. (2015). *Sexting: Gender and Teens*. Massachusetts, USA: Springer.
- Del Moral Pérez, M. E., Martínez, L. V., Tosina, R. Y., y Esnaola, G. (2012). Evaluación y diseño de videojuegos: generando objetos de aprendizaje en comunidades de práctica. *Revista de Educación a Distancia*.33 1-17
- García Jorba, J. M. (2000). *Diarios de campo*. Madrid, España: CIS
- García, T. y González, M. (2011). E-learning en mundos virtuales 3D. Una experiencia educativa en Second Life. *Revista ICONO14. Revista científica de Comunicación y Tecnologías emergentes*, 9(2), 39-58.
- Gregori, E., Majós, T., Onrubia, J., y Aguado, G. (2008). *Cómo valorar la calidad de la enseñanza basada en las TIC: Pautas e instrumentos de análisis*. Graó.
- Grings, E. S., Trein, D., y Oliveira, C. (2009). The metaverse: Telepresence in 3D avatar-driven digital-virtual worlds. @ Tic. *Revista d'innovació educativa*, (2), 26-32.
- Horner Miller, J. (2016). ARCS Model *Instructionaltechnologist101.wordpress.com*. Recuperado el 5 de junio de 2016, de <https://instructionaltechnologist101.wordpress.com/tag/arcs-model/>
- Keller, J. (2016). *arcsmode.ipower.com*. Recuperado el 6 de junio de 2016, de <http://www.arcsmodel.com/>
- Keller, J. M. (2009). *Motivational design for learning and performance: The ARCS model approach*. Florida, USA: Springer Science y Business Media
- Kelton, A.J. (2008). Virtual Worlds? Outlook Good. *Educause Review*. 43 161-163

- Kessem, L. (2012). Colombia es uno de los países más atacados en el ciberespacio. *Semana.com*. Fecha de consulta: 16 de mayo de 2016, disponible en: <http://www.semana.com/enfoque/enfoque-principal/articulo/colombia-paises-mas-atacados-ciberespacio/263650-3>
- Koehler, M., y Mishra, P. (2009). What is technological pedagogical content knowledge (TPACK)?. *Contemporary issues in technology and teacher education*, 9(1), 60-70.
- Kovalchick, A., y Dawson, K. (Eds.). (2003). *Education and technology: An encyclopedia..* California, USA: Abc-clio
- Lenhart, A. (2009). Teens and Sexting. Fecha de consulta: 16 de mayo de 2016. Recuperado de: http://ncdsv.org/images/PewInternet_TeensAndSexting_12-2009.pdf
- Lima, J. R., y Capitão, Z. M. A. (2003). *e-Learning e e-Conteúdos*. Centro Atlántico.
- Litwin, E. (2005). *Tecnologías educativas en tiempos de Internet*. Buenos Aires: Amorrortu.
- López Camps, J. (2005). *Planificar la formación con calidad*. Barcelona, España: Editorial Praxis.
- López, R. G. (2011). Los Nativos Digitales Y Sus Metaversos. *Educación y Sociedad*. 10 (5) 3-11
- Márquez, I. (2010). La simulación como aprendizaje: educación y mundos virtuales. *Documento presentado en el II Congreso Internacional de Comunicación* (3). España.
- Méndez-Ibáñez, E., Martí-Parreño, J., Queiro-Ameijeiras, C., y Giménez-Fita, E. (2015). El uso de la gamificación en la educación superior: el caso de Trade Ruler. *XII Jornadas Internacionales de Innovación Universitaria Educar para transformar: Aprendizaje experiencial*. 95-102
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Ley 1273 de 2009 - Mintic.gov.co*. Fecha de consulta 1 abril de 2016. Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-3705.html>
- Monterroso, E., y Romero, R. E. (2011). Enseñanza práctica en 3D: juicio virtual, *Revista de innovación educativa* 54(1), 46-54.
- Moreira, M. A. (2000). *Aprendizaje significativo: un concepto subyacente*. Madrid, España: Morata.
- Namakforoosh, M. N. (2000). *Metodología de la investigación*. Balderas, México: Editorial Limusa.

- Naya, V., López, R., y Ibáñez, L. (2012). Metaversos formativos. Tecnologías y estudios de caso/educational metaverses. *Technology and case studies. Vivat Academia*, 14(117), 121-144.
- New Media Consortium [NMC] (2016). *Higher Education Edition. (2016). The New Media Consortium*. Recuperado el 14 de mayo de 2016, de <http://www.nmc.org/publication/nmc-horizon-report-2016-higher-education-edition/>
- Pere, C. P. y Oliver T. S. (2015). *Internet negro*. Madrid, España: Grupo Planeta.
- Pew Research Center. (2009). *Teens and Sexting*. Pew Research Center: Internet, Science y Tech. Recuperado el 6 de junio de 2016, de <http://www.pewinternet.org/2009/12/15/teens-and-sexting-2/>
- Piscitelli, A. (2009) Nativos digitales. Dieta cognitiva, inteligencia colectiva y arquitecturas de la participación. Montevideo, Uruguay: Santillana.
- Reigeluth, C. M. (Ed.). (2013). *Instructional design theories and models: An overview of their current status*. Routledge.
- Rué, J. (2009). *El aprendizaje autónomo en educación superior*. Madrid, España: Narcea Ediciones.
- Shambhu, B. T. (2016). *WhatsApp: Unlocking The Goldmine*. New Delhi, India: Educreation Publishing.
- Stake, R. E. (1998). *Investigación con estudio de casos*. Madrid, España: Ediciones Morata.
- Stephenson, N. (1992). *Snow Crash [1992]*. New York, USA: Bantam-Random.
- Tapia, J. A. (2005). Motivación para el aprendizaje: la perspectiva de los alumnos. En María Pérez Solís y Alicia Rivera Otero (Ed) *La orientación escolar en centros educativos*. España: Ministerio de Educación y Ciencia. (p. 209-237)
- UNICEF. (2014). *Grooming: Una guía para adultos*. Recuperado de: https://books.google.com.co/books?id=1XURBgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- Unity - Game Engine. (2016). *Unity3d.com*. Recuperado el 16 de mayo de 2016, de <http://unity3d.com/es>
- Universidad de Cundinamarca. (2015). *PEI: Universidad de Cundinamarca*. Recuperado de: <http://www.unicundi.edu.co/documents/rectoria/PEI.pdf>
- Voutssas, M. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*, 24 (50), 127-155.

ANEXOS

Anexo 1: Formato de evaluación del material educativo.

1. Identificación y características generales del material.
 - a. Nombre del material: Mundo Virtual de conceptos de Seguridad Informática
 - b. Autor: Juan Camilo Gutiérrez P.
 - c. URL: Archivo ejecutable localmente
 - d. Fecha de edición y versiones: Mayo de 2015
 - e. Destinatarios del material: Estudiantes de Tecnología en Informática
 - f. Temática: Seguridad Informática
 - g. Objetivos:
 - ✓ Identificar riesgos en las redes sociales, mediante un tour virtual elaborado en Unity.
 - ✓ Ilustrar mediante el RED diferentes tipos de ataques informáticos.
 - ✓ Reconocer algunas buenas prácticas para minimizar los riesgos en las redes sociales y los ataques informáticos
 - i. Se describen: Si X No___
 - h. Contenidos:
 - i. Se describen: Si X No___
 - ii. Cuáles son:
 - ✓ Riesgos en las redes sociales.
 - ✓ Ataques informáticos.
 - ✓ Buenas prácticas.
 - i. Apoyo al docente: Si X No___
 - j. Apoyo tecnológico: si
 - k. Recomendaciones sobre su uso en procesos formativos: Si X No___
2. Accesibilidad, facilidades de uso y fiabilidad.
 - a. Acceso: Internet X CD X DVD___
 - b. Equipo necesario para accederlo:

Computador con Sistema operativo Windows 7 o superior.

c. Calidad de la imagen:

Muy deficiente	Deficiente	Aceptable	Buena	Muy buena
				X

d. Calidad del sonido:

Muy deficiente	Deficiente	Aceptable	Buena	Muy buena
				X

e. Desajustes en la correspondencia entre imágenes y sonido: Si ___ No X

f. Facilidad de uso del sistema de navegación

MUY BAJA ___ ACEPTABLE ___ ALTA X MUY ALTA ___

Si la valoración es muy baja, baja ó aceptable, indicar las dificultades y a qué características del sistema de navegación cabe atribuir las: _____

g. Velocidad de navegación

MUY BAJA _____ ACEPTABLE X ALTA ___ MUY ALTA _____

Si la valoración es muy baja, baja ó aceptable, indicar si la lentitud es generalizada o se produce únicamente en algunas zonas: _____

3. Características Multimedia del Material

a. Lenguajes utilizados en la presentación de los contenidos

Item	SI	NO
Texto oral	X	
Texto escrito	X	
Imágenes fijas	X	
Imágenes en movimiento	X	
Gráficos	X	
Mapas conceptuales		X
Sonido	X	
Lenguajes simbólicos (lenguaje matemático)		X

b. Calidad técnica de las imágenes

Muy deficiente	Deficiente	Aceptable	Buena	Muy buena
				X

c. Tipos de letras y caracteres tipográficos en general:

Muy deficiente	Deficiente	Aceptable	Buena	Muy buena
			X	

Por qué: El tipo de letra y fuente es adecuada y se entiende

d. Calidad técnica del sonido locución:

Muy deficiente	Deficiente	Aceptable	Buena	Muy buena
				X

e. Calidad técnica de la integración sonido-imagen (audio y video se perciben como un todo):

Muy deficiente	Deficiente	Aceptable	Buena	Muy buena
			X	

f. Frecuencia global de los diferentes lenguajes utilizados en la presentación de los contenidos (en el conjunto del material)

Item	Muy baja	Baja	Media	Alta	Muy alta
Texto oral				X	
Texto escrito				X	
Imágenes fijas			X		
Imágenes en movimiento					X
Gráficos					X
Sonido / música					X

g. Utilización combinada de diferentes lenguajes en la representación de contenidos

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
			X	

4. Objetivos y contenidos

a. El material incluye una formulación explícita de los objetivos formativos perseguidos mediante su utilización o estudio

<u>SI</u>	<u>NO</u>
X	

b. Tipos de contenidos abordados en el conjunto del material

	Totalmente	Muy poco	Relativamente	Bastante	Muy frecuente
--	------------	----------	---------------	----------	---------------

	ausentes	frecuen tes	frecuentes	frecuen tes	ntes
Hechos, datos			X		
Conceptos, principios, teorías					X
Procedimientos,			X		
Actitudes, valores				X	

c. Complejidad del conjunto de los contenidos del material

Muy baja	Baja	Media	Alta	Muy alta
		X		

5. Presentación, organización y secuenciación de los contenidos.

a. Presentación de una visión de conjunto de los contenidos del material

SI	NO
X	

b. Correspondencia entre la visión de conjunto de los contenidos del material y su desarrollo efectivo

Muy escasa	Escasa	Aceptable	Alta	Muy alta
			X	

c. Transparencia, visibilidad y claridad de la organización de los contenidos del material en su conjunto (organización por fases, apartados, puntos, temas, núcleos... transparente, clara y visible)

Muy escasa	Escasa	Aceptable	Alta	Muy alta
		X		

d. Tipos de secuencias presentes en la organización de los contenidos del material en su conjunto (no excluyentes)

	SI	NO
Secuencia global: De lo simple a lo complejo		X
Secuencia global: aportación de información, explicación-ilustración, ejemplificación	X	
Secuencia global: aportación de información, explicación-problemas		X
Secuencia global de: resolución de problemas		X

e. Ritmo en la presentación de los contenidos

Muy inadecuado	Inadecuado	Aceptable	Adecuado	Muy adecuado

			X	
--	--	--	---	--

6. Tratamiento instruccional de los contenidos

- a. Elementos instruccionales presentes en el material y en las unidades, temas, bloques, módulos o partes en que está organizado

	Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
Elementos de refuerzo de la comprensión de los contenidos (esquemas, gráficos, señalizaciones, animaciones, simulaciones, ejemplificaciones)					X
Interpelaciones al estudiante para que anticipe, prevea, reflexiones, relacione			X		
Mensajes de refuerzo emocional			X		
Mensajes de refuerzo cognitivo			X		
Ejemplos, situaciones, problemas, elementos. relevantes del medio socio cultural de los aprendices				X	
Elementos de sorpresa o divertidos que rompen la monotonía y la rutina de la explicación			X		

- b. El material incluye sugerencias de actividades o ejercicios sobre los contenidos presentados

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
		X		

- c. El material incluye sugerencias o propuestas de ampliación o profundización de los contenidos presentados

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
		X		

- d. El material incluye propuestas de actividades de autoevaluación

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
		X		

- e. El material incluye las coordenadas (correo electrónico, espacio web.. para plantear dudas y preguntas a un tutor)

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente

X				
---	--	--	--	--

Estrategias discursivas

- f. Hay uso de primera persona del plural

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
X				

- g. Recapitulaciones, resúmenes o síntesis de los contenidos

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
		X		

- h. Alusiones a experiencias, conocimientos, vivencias, no específicamente relacionados con los contenidos del material que “supuestamente comparten los aprendices”

Nunca	Casi nunca	A veces	Frecuentemente	Sistemáticamente
			X	

7. Usos del material en procesos formativos.

- a. Adecuación del material globalmente considerado para su uso en procesos formativos de autoaprendizaje o en procesos formativos presenciales y semipresenciales, según proceda

Muy inadecuado	Inadecuado	Aceptable	Adecuado	Muy adecuado
				X

- b. Calidad del material globalmente considerado en la perspectiva de su utilización en procesos formativos de autoaprendizaje o en procesos formativos presenciales y semipresenciales, según proceda

Muy baja	Baja	Media	Alta	Muy alta
				X

A continuación, se presenta el Story Board del material educativo que ilustra las fases del tour virtual y los escenarios que se plantearon inicialmente.



En la siguiente imagen se ilustra un primer bosquejo del mundo virtual y los diferentes senderos.



A continuación, se definieron los elementos del primer y segundo nivel a incorporar en el tour virtual con la respectiva explicación.

A PARTIR DE LA PANTALLA EL MAPA	
Elementos de primer nivel: <ul style="list-style-type: none"> • Ingreso • Cuestionamientos • Riesgos en las redes sociales • Ataques Informáticos • Evaluación interactiva 	Elementos segundo nivel: <ul style="list-style-type: none"> • Sexting • Grooming • Phishing • Hoax • Spoofing • Herramientas para recuperación de de datos. • Quiz Interactivo
Ruta sugerida	El usuario ingresa al mundo virtual que se ambientará en una isla, en donde encontrará, unos cuestionamientos sobre los temas a tratar, posteriormente debe buscar dos locaciones, la primera, relativa al tema de riesgos en las redes sociales y la segunda, trata acerca de conceptos de ataques informáticos e informática forense, en cada uno de los dos escenarios existen algunos objetos educativos relativos al tema. Finalmente se dispondrá de una evaluación interactiva, donde se indagará al usuario los conocimientos adquiridos.

En el escenario 1 se enfoca en los riesgos existentes en las redes sociales, y en la etapa de diseño se propuso incorporar recursos educativos como videos y presentaciones, que ilustran al estudiante las características y ejemplos de los riesgos. En las dos siguientes imágenes se observan los conceptos de Sexting y Grooming para dicho escenario.

ESCENARIO 1 - RIESGOS EN REDES SOCIALES - SEXTING

Descripción gráfica:



En el primer salón del escenario de riesgos en redes sociales el usuario encontrará una pantalla en la cual después de accionar un botón se reproducirá un video, relativo al tema de sexting, además encontrará en otra pantalla, una animación acerca de datos llamantes de sexting en américa latina y por último, una presentación de como evitar el sexting en 5 pasos, la categoría que puede consultarse en el siguiente enlace:

<https://www.youtube.com/watch?v=Gp4ZV0YmXuY>

Audio:

Se escucha el audio de fondo, mientras que no este ejecutado por el usuario.

Q2 - Álbum Minimal attitude - q side EP por Moby!

Loop de toda la canción

puede descargar desde acá:

<https://www.jamendo.com/es/track/319575/q2>

Contenidos – textos:

"Sexting es el acto de enviar mensajes o fotografías sexualmente explícitas por medios electrónicos, especialmente entre teléfonos celulares".

(tomado de: <http://081y/1sIRn>)

ESCENARIO 1 - RIESGOS EN REDES SOCIALES - GROOMING

Descripción gráfica:



Audio:

Se escucha el audio de fondo de un video dramatizado de un caso de grooming. Se puede descargar desde acá:

<https://www.youtube.com/watch?v=C4Tp15YQsk>

Descripción de acciones:

En el segundo salón del escenario de riesgos en redes sociales el usuario encontrará diversos objetos de aprendizaje, que se presentarán en pantallas que se activarán cuando la persona lo desee, describiendo en la primera el tema de grooming, además, encontrará en otra pantalla, una presentación de como evitar el grooming. El video puede consultarse en el siguiente enlace:

<https://www.youtube.com/watch?v=C4Tp15YQsk>

Contenidos – textos:

“Grooming es el acto de enviar mensajes o fotografías sexualmente explícitas por medios electrónicos, especialmente entre teléfonos celulares”.

[tomado de: <http://www.protecciononline.com/19988fng&Buscador=0&vicon=y=2>]

En el segundo escenario se propone definir mediante algunos recursos educativos digitales los contenidos relativos a conceptos de Seguridad Informática: Hoax, Phishing y Spoofing. El siguiente gráfico corresponde al componente en el Story Board.

ESCENARIO 2 - ATAQUES INFORMÁTICOS HOAX PHISHING SPOOFING

Descripción gráfica:



Audio:

Se escucha el audio de fondo, mientras que no este ejecutado por el usuario.

Q2 - Álbum Minimal attitude - q side EP por Moby!

Loop de toda la canción

puede descargar desde acá:

<https://www.jamendo.com/es/track/319575/q2>

Descripción de acciones:

En el segundo escenario de ataques informáticos el usuario está en un balcón en el cual aparecerán diversos objetos de aprendizaje que ilustrarán los temas de Phishing, hoax y spoofing.

Contenidos – textos:

“La seguridad en Internet es muy importante y esta seguridad depende de algunos factores clave como la utilización de una contraseña segura, la reducción de informaciones privadas que compartimos en Internet y con quién o quiénes interactuamos en la Web.”.

[tomado de: <http://www.protecciononline.com/tutoriales-para-crear-contraseñas-seguras-evitar-el-phishing-y-spoofing/>]

Inicialmente se plantearon las actividades dentro del material como se evidencia a continuación.

ESCENARIO 1 - RIESGOS EN REDES SOCIALES - ACTIVIDAD

Descripción gráfica:



Audio:

Se escucha el audio de fondo, mientras que no este ejecutado por el usuario.

Q2 - Álbum Minimal attitude - q side EP por Moby!

Loop de toda la canción

puede descargar desde acá:

<https://www.jamendo.com/es/track/319575/q2>

Descripción de acciones:

Como Actividad del segundo escenario, se le pedirá al usuario que dispore a unos globos que se identifican cada uno a una posible respuesta, en función de algunas preguntas solicitadas.

Foto tomada de:
http://pixabay.com/static/uploads/photo/2014/01/10/14/33/hot-air-balloon-241642_640.jpg

Contenidos - textos:

"HOAX, PHISHING, SPOOFING Y DEEP WEB".

Anexo 3: Formato de Diario de campo.

<i>Diario de Campo No. 1</i> <i>Fecha: Octubre 6 de 2015</i> <i>Lugar: Sala de Sistemas No. 2 Universidad de Cundinamarca</i> <i>Tema: Tour Virtual acerca de Riesgos en las redes sociales y ataques informáticos</i>	
<i>PROPÓSITO</i>	<i>DESCRIPCIÓN</i>

Anexo 4: Cuestionario.**CUESTIONARIO****OBJETIVO:**

Determinar cómo puede un mundo virtual influir en el aprendizaje de conceptos de Seguridad Informática.

Duración: 15 min.

Por favor diligenciar todas las preguntas y brindar la mayor información posible, la cual es muy importante para alcanzar el objetivo.

1. Nombra 5 aspectos positivos de la actividad
2. ¿Qué ventajas encuentras en el tour virtual en el aprendizaje de conceptos de seguridad informática?
3. ¿Qué desventajas encuentras en el tour virtual en el aprendizaje de conceptos de seguridad Informática?
4. Nombra al menos 5 conceptos aprendidos en la actividad.
5. ¿Qué inconvenientes de uso tuviste en el recorrido del tour virtual?
6. ¿Cómo te parecieron los temas abordados en la actividad? Justifique su respuesta
7. ¿Qué diferencias encuentras al usar esta pedagogía con la tradicional?
8. ¿Qué riesgos existentes en las redes sociales aprendiste?, nombra al menos 2.
9. ¿En qué consideras que te puede aportar los conceptos de seguridad informática y los riesgos en las redes sociales?
10. ¿Qué elementos agregarías al tour virtual?

Anexo 5: Entrevista.

ENTREVISTA

OBJETIVO:

Determinar cómo puede un mundo virtual influir en el aprendizaje de conceptos de Seguridad Informática.

Pregunta No.1

Entrevistador: ¿Cómo te pareció la actividad?

Estudiante:

Pregunta No.2

Entrevistador: ¿Qué inconvenientes tuviste en el recorrido del tour virtual?

Estudiante:

Pregunta No.3

Entrevistador: ¿Conoces los riesgos existentes en las redes sociales?

Estudiante:

Pregunta No.4

Entrevistador: ¿Qué diferencias encuentras al usar esta pedagogía con la tradicional?

Estudiante:

Pregunta No.5

Entrevistador: ¿Qué ventajas encuentras en el tour virtual en el aprendizaje de conceptos de seguridad informática?

Estudiante:

Pregunta No.6

Entrevistador: ¿Qué desventajas encuentras en el tour virtual en el aprendizaje de conceptos de seguridad informática?

Estudiante:

Pregunta No.7

Entrevistador: ¿Qué elementos agregarías al tour virtual?

Estudiante:

Pregunta No.8

Entrevistador: ¿Qué conceptos aprendiste en este ejercicio?

Estudiante:

Anexo 6: Cuadro de comentarios de segmentos de análisis de categorías.

COMENTARIO	SEGMENTO DEL CUESTIONARIO
Aspectos positivos de la actividad.	<i>El juego es pedagógico. Los temas son interesantes</i>
Innovación pedagógica	<i>Se muestra la información de forma diferente e innovadora,</i>
En algunas ocasiones se torna monótono.	<i>Variar la forma de enseñar los temas, y después de un tiempo se pone monótono.</i>
Le interesaron especialmente los riesgos en las redes sociales.	<i>Sexting, grooming, phishing y Cyberbulling</i>
Dificultad con la interacción de los videos.	<i>No sabía cómo empezar los videos</i>
Entendimiento de los conceptos vs fijación de los mismos	<i>Muy interesantes, conocía de algunos pero no sabía cómo se llamaban</i>
Consideran la herramienta como divertida	<i>Es más divertida,</i>
Aporte en el desempeño laboral	<i>Como estudiante de Ingeniería de Sistemas es necesario conocer los temas del tour, para el día a día y en el desempeño laboral.</i>
Interacción con personajes	<i>Otras actividades e interacción con personajes.</i>
Actividad Divertida	<i>Fue una actividad con la didáctica del juego muy divertida, con temas interesantes.</i>
La temática es una ventaja	<i>Los temas tienen que ver con tecnología y los videos interesantes.</i>
Implementar la dinámica del juego	<i>Integrar actividades de juego en la actividad.</i>
Aprendizaje principal: Riesgos en las redes sociales	<i>Sexting, spoofing y Cyberbulling</i>
Mejorar el cierre del tour virtual	<i>No identifique el final del tour.</i>
Libertad en el recorrido (Ventaja)	<i>El mundo virtual se puede recorrer de manera libre seleccionado el módulo que más considere conveniente, y el profesor no dicta el tema directamente.</i>
Importancia de la Privacidad e Intimidad	<i>Es muy importante conocer estos conceptos, por temas relacionados con la privacidad de la información e intimidad de cada persona.</i>
Temas a incluir en posteriores estudios	<i>Incluir otros temas de seguridad Informática, como informática forense, y como detectar los ataques informáticos y como enfrentarlos.</i>
Calidad gráfica y escenarios	<i>Los gráficos son muy buenos, los videos muy interesantes, los escenarios modernos y la duración de la actividad es adecuada.</i>
Los videos como herramienta adicional en el tour virtual	<i>Es una forma diferente de aprender, y los videos muestran con ejemplos reales.</i>

Dificultad de actividades en inglés	<i>A pesar de los subtítulos, los videos en inglés dificultan la comprensión de la totalidad de los conceptos.</i>
Uso de las redes sociales	<i>Muy interesantes los temas porque nosotros los jóvenes utilizamos mucho las redes sociales, y desconocemos los peligros y el tipo de personas que quieren apoderarse de nuestra información personal</i>
Didáctica innovadora	<i>Es diferente porque estamos acostumbrados a que los profesores usen los tableros o el videobeam, pero nunca he usado este tipo de software.</i>
Aporte en aprendizaje de la protección de la información personal	<i>Para proteger la información personal y aplicarlas en el trabajo.</i>
Mejora para llevar a dispositivos móviles	<i>Que se pudiera realizar el tour desde el celular.</i>
Disponibilidad de los contenidos	<i>Los contenidos pueden verse las veces que se quiera, los gráficos son de gran calidad y la temática es muy interesante y se presentan de una manera diferente.</i>
Dificultad con espacios cerrados	<i>Acostumbrarse a recorrer los espacios en tres dimensiones y los espacios son un poco cerrados y algunos oscuros.</i>
Elaboración de una guía interactiva	<i>Identificar el ingreso a la edificación, no existe una guía interactiva durante el tour.</i>

Anexo 7: Respuestas Cuestionario**Nombra 5 aspectos positivos de la actividad (16 respuestas)**

información nueva en temas relacionados a: privacidad, seguridad, redes sociales, tipos de amenazas. seguridad en la familia, información personal, trafico de pornografía en menores , falsificación en documentos, redes seguras

primero pude identificar claramente los diferentes tipos de ataques, tanto como con viros como en las redes sociales donde se presenta diferente abusos. segundo a partir de estas charlas que mostraban en los videos podemos hacer varias acciones para evitar al maximo estos ataques y tambn abusos como en el caso de las redes sociales. como tercero puedo identificar que estas recomendaciones y acciones no solo es para nosotros sino tambn podemos transmitir esta informacion a familiares, extender esta informacion. en cuarto punto es tener una idea de como por medio de un juego podemos promover esta informacion de forma mas recreativa. como ultimo punto somos futuros ingenieros de sistemas a los cuales nos enfrentaremos a estos ataques pero ya a un nivel mas alto, como por ejemplo la seguridad de una empresa y tambien el dia de mañana tener la cultura de evitar hacer estos ataques a la compañías, como acabe de resaltar tener cultura de no hacerlo y ademas de que nos enfrentariamos a situaciones que son castigables legalmente.

Ingeniosa, creativa, llamativa, interesante y acorde al tema

conocimientos con respecto a los temas de seguridad informatica, ayuda a preocuparse por los riesgos que se corren en la internet, brinda una ayuda didactica para el usuario, explica temas que resultan utiles e importantes.

aporte de conocimiento sobre como protegernos de ataques informáticos, conocimiento sobre las principales técnicas de ataques, importancia del manejo de la información, a través del juego se hace muy dinámico el aprendizaje y la forma de como se pueda ya saber la información de una persona y como puede ser a futuro

Debe mantener la 1. Confidencialidad de los datos personales, 2. Integridad

Muy dinámico e interactivo, aclaración de conceptos, ejemplos de la vida real, expositores con mucha experiencia y varios ejemplos

nuevos conocimientos, importancia de la privacidad, tipos de ataques, vulnerabilidades en las redes sociales, modo interactivo para aprender.

realidad, navegación segura, revelación de las redes sociales, protege la informacion

temas actualizados y interés forma diferente y llamativa de aprender conocer una nueva herramienta para hacer presentaciones interacción a manera de vídeo juego

1. informacion sobre antivirus 2. las conferencias buscan dar conciencia de la nuevas tecnologias 3. tener pendiente como la informacion esta disponible a todo el mundo 4. la importancia de encriptar la informacion 5. proteger nuestra identidad.

1.nos brindan gran información de los riesgos informáticos actuales 2.nos da una idea de la importancia que tiene la información 3.nos da una idea de la importancia de la privacidad 4.nos concientiza acerca de lo importante que es mantener nuestra información personal privada 5.Nos brinda o nos abre un campo de acción que como ingenieros podemos aprovechar

información claridad importancia interesante creativo

Informar, combatir los cibercrimenes malware, educar, despertar conciencia sobre los peligros en la red, incentivar el valor a la informacion personal, diversion

Dinámica, Visualización de los vídeos, información por secciones

2. ¿Qué ventajas encuentras en el tour virtual en el aprendizaje de conceptos de seguridad informática?(16 respuestas)

Prevenir sobre los posibles ataques informaticos

Se puede utilizar en cualquier lugar y por diferentes tipos de usuarios y/o edades

La importancia de proteger la información, Tolerancia a fallos, Respaldos (backup), Métodos de Protección Contra Intrusiones Remotas

las ventajas son muchas como acabo de resaltar, basicamente es tener idea de los ataques a los que nos enfrentamos a diario y las posibles acciones que podemos realizar para evitarlo. ademas de esto nos enfrentamos a una sociedad adolescentes donde los niños ya estan en esta redes sociales y como familiares y como ejemplo les podemos hablar sobre estos temas para evitar estos abuso y o ataques.

el aprendizaje de forma interactiva genera un mayor impacto e interes en estos temas.

la principal ventaja es que da el conocimiento para protegernos de la forma mas básica de los grandes ataques que se realizan a través de la web

un tema muy interesante para seguir estudiando y ponerle mas atención, personalmente me gusta el tema de la seguridad informática y la idea es enfatizar mas en los temas de seguridad informática.

para nuestra carrera es muy importante conocer todos los riesgos a los que podemos conocer el incluso caer.

Los conceptos que se comparten en la sala

es una manera interactiva, divertida y diferente de aprender estos temas, me parece que es una buena herramienta para el aprendizaje

Una forma muy divertida de aprender, aprendizaje efectivo, innovador, forma directa de aprendizaje son temas que se complementan, nos brindan datos reales, y las formas como estamos somos vulnerables

encuentro que es una manera mas didactica y motivante para las personas en especial para los niños que acceden a la web de manera continua

como proteger nuestra información ya que es muy vulnerable por las redes sociales del momento

que es un entorno interactivo y entretenido captando la atención del usuario y concentrándolo en el tema ademas de brindar mucha información tanto en vídeos como en carteleras que nos informan sobre esta realidad

encriptar la informacion, saber las formas de virus que hay, como actuan, manejas como acceder a otras cuentas.

3. ¿Qué desventajas encuentras en el tour virtual en el aprendizaje de conceptos de seguridad Informática?(16 respuestas)

Ninguna

Cansancio con respecto a lo videos

ninguna, solo agregaria control de pausa en los videos

la falta de controles para los videos (adelantar atrasar pausa)

Algunos videos TED son muy largos

en algunos casos distrae

esta bien como tema de cultura general para estar todos informados, mas animacion estaria bien vídeos con subtítulos.

Muy breve la información presentada en las dos primeras salas

faltaron mas temas como tipos de virus

revela que son muy fáciles las claves que utiliza la mayoría de las personas y cualquier persona con la información básica de otra le puede empezar a jaquear la cuentas electrónicas

ninguna

ninguna

ninguna

ninguna

en cuanto a la interfaz le hace falta renderizar y también ajustar los controles

4. Nombra al menos 5 conceptos aprendidos en la actividad. (16 respuestas)

spoofing phishing sexting hoax

1.pgp 2. PROTONMAIL 3. BOB 4.SEXTING 5.HOAX

phishing, grooming, información pública, sexting, TED, privacidad

encriptación manipulación de la información reproducción de virus informáticos imágenes eróticas sin ningún tipo de protección

1.seguridad de la información 2.privacidad 3.phishing 4.hacking 5.basic16

sixting, ted, phishing, spoofing, oast

privacidad, grooming, TED, phishing, sexting.

malware, phishing, extorsión sexual, suplantación de receptor, organizaciones de cibercrimen

Ted, Phishing, sexting, grooming, spoofing

Hoax, Phishing, Troyano, virus, sexting

vulnerabilidad de la información, phishing, sexting, grooming

seguridad informática, phishing, pornografía, cibersexo, hacking

contraseñas phishing ataques informáticos peligro en redes sociales riesgos en el correo

spoofing, grooming, sexting, hoax, phishing

sexting pushing spoofing grummin hoax

Phishing, sexting, seguridad informática, encriptación, password

5. ¿Qué inconvenientes de uso tuviste en el recorrido del tour virtual? (16 respuestas)

bueno en cuanto a teoría e información fue clara algunas aclaraciones al principio fueron clave para saber llevar la organización. muy buenas gráficas.

no reproducen los videos con facilidad se pierde con facilidad de la ruta

es un poco complejo y confuso en ocasiones reproducir los videos

no tener control sobre la pausa del video

ninguno, algo más de interacción

El puntero del mouse se movía demasiado rápido

la sensibilidad del mouse

AL BLOQUEAR SE DEBE SALIR Y REINGRESAR DE NUEVO,

tuve que cerrar el programa y volverlo a abrir por que no me reproducía un video y sería muy bueno que los dejara pausar, adelantar y rechazar

Sensibilidad en el mouse

muy sensible

sensibilidad de movimientos muy alta por lo tanto complica desplazamientos.

La sensibilidad de la cámara es muy alta

Algunos vídeos no arrancan fácilmente

La sensibilidad del movimiento y reproducir los movimientos

inconvenientes en cuanto al manejo del meta verso o mundo virtual, falta calibrar el mouse

6. ¿Cómo te parecieron los temas abordados en la actividad?

Justifique su respuesta(16 respuestas)

me parecio muy interesante y dinamica y pues para el momneto la informacion fue basica pero entendible

Interesantes ya que debemos saber sobre la seguridad informatica.

Son temas de vital importancia ya que todos estos temas se manejan en la actualidad

BIEN , EN LAS CONFERENCIAS NOS VISIONAN PARA DONDE NUESTRA INFORMACION .

muy interesantes, son temas que se están viviendo en la actualidad y debemos conocerlos, y transmitir esta informacion

importantes ya que nos hablan de la importancia de proteger nuestra información y lo vulnerables que estamos de nuestra información ante las redes sociales

son temas puntuales y con vídeos bien didacticos

muy interesantes, ya que esta es la linea de profecion en la cual quiero basarme y seguir por tal motivo me gusto mucho esta actividad

De bastante importancia porque es bueno tener conocimiento sobre lo ocurre cuando usamos las redes sociales

Excelente, me parece que el tema de sexting se puede implementar perfectamente en escuelas colegios para evitar que los jóvenes caigan en esta trampas.

los temas son validos y son de la realidad lo cual es pertinente puesto que la web ofrece una sin infinidad de información pero hay otras personas que se aprovechan del desconocimiento de las mismas y sacan ventaja de ello

de vital importancia ya que el tema afecta drasticamente a todos los usuarios de internet en especial aquellas que no tengan ningun conocimiento sobre estos fenomenos

Apropiados, abarcan en gran medida varios temas relacionados con la seguridad informática.

bastante buenos, debido a que no se tienen acceso todos los dias a los temas vistos en el tour virtual ya que no se habla mucho de esto.

interesantes muy acuerdo a nuestra carrera de sistemas

Me parecieron muy buenos e importante ya que hoy en día la mayoría de las personas pasan mucho tiempo en las redes sociales y no sabemos o no nos damos cuenta que la información que ponemos allí la podría ver cualquier persona

7. ¿Qué diferencias encuentras al usar esta pedagogía con la tradicional?(16 respuestas)

es mas llamativa, menos monotono.

no se tiene contacto con el expositor pero se compensa al ser muy interactivo

que esta metodología nueva es mucho mas interesante y interactiva que la típica cátedra de clase.

es a lo que se tendría que apuntar, pero el tema va en la manera que cada persona aborde temas de aprendizaje, personalmente aprendo de forma mas didáctica, habrá mas gente que le guste otra cosa.

Se aprende interactuando

Es una pedagogía más llamativa que no aburre como sentarse en un salón a escuchar a alguien o verlo como llena tableros.

que esta resulta más motivante y didáctica para el usuario

QUE EL AMBIENTE VISUAL ES DIDÁCTICO DINÁMICO.

brinda más interés a la hora de obtener el conocimiento, se hace más llamativo evita caer en el aburrimiento de solo leer copias o ver presentaciones planas.

es muy atractiva al ser de tipo video juego

dinámica, con tendencia a la realidad de los video juegos

es más interactivo y divertido

es un estilo libre y dinámico lo que no hace lo tradicional, uno puede escoger la velocidad en la que aprende

Hay muchas diferencias ya que en esta pedagogía se simulaba un ambiente de juego y creo que nuestro cerebro aprende mucho mejor así desde lo más básico y dinámico

es una forma más atractiva que permite generar interés en los temas a tratar.

Es intuitiva en el sentido de que simula el recorrido por una variedad de salas donde se pueden escoger los temas de agrado

8. ¿Qué riesgos existentes en las redes sociales aprendiste?, nombra al menos 2. (16 respuestas)

muchas personas pueden revisar la información con gran facilidad y conocer mucha información importante

las personas pueden utilizar estas redes sociales como abuso sexuales para los adolescentes y también puede ser engaños para obtener cuentas bancarias

perdida de la privacidad, reconocimiento facial y big data

sexting, phishing

1. clonación de fotos para usos indebidos 2. uso de nuestra información para malos fines esto se puede hacer a través de virus y malware

sixting grummin

Sexting y droming

extorciones por captura de imágenes sexuales, información vulnerable, fotos de usuarios usadas de forma malintencionada, exposición al big data

hackeo, phishing

subplantación mi ubicación puede obtenerse con facilidad con un dato de algún usuario se puede saber con certeza la información del usuario con reconocimiento de rostros y demás

subir fotos con contenido de desnudos no conocer a mis "amigos" que tengo en mis redes sociales

Sexting, phishing

1. LA INFORMACIÓN ESTÁ DESPROTEGIDA 2. LA INFORMACIÓN ESTÁ EXPUESTA A TODO EL MUNDO.

Tener cuidado con la información que se sube Spoofing, sexting, hoax, phishing

sexting, grooming

sexting, grooming

9. ¿En qué consideras que te puede aportar los conceptos de seguridad informática y los riesgos en las redes sociales? (16 respuestas)

Me sirven para tener cuidado con las imágenes o información que se publica en las redes sociales

conocimientos para proteger nuestra información cambiar claves constantemente y utilizar diferentes caracteres

tener conocimiento, para no caer en las diferentes actividades fraudulentas

en tener la precaución de compartir mi información en las redes sociales

en mucho ya que en la vida cotidiana cometemos muchos errores y fallas que ponen en riesgo nuestra información personal

EN NUESTRO DIARIO VIVIR

en todo ámbito por que actualmente todo se mueve en relacion a estos temas

En ser mas precavido con los password que se colocan y en no publicar demasiada información en las redes sociales.

tener en cuenta el manejo de la seguridad para futuros desarrollos de app,

Aumenta el numero de obstaculos entre mi informacion y la delincuencia en la red

Prevenir de los atacantes

Ser un poco mas precavido con la informacion que dejo en mis redes sociales

estos consejos me sirven para proteger mejor mi equipo y mi informacion

conciencia con la información que se brida en las redes sociales.

en saber que sitios seguros visitar para consultas, descargas y compras

ayuda a no dar información por la web ademas muestra la manera en la que pueden capturar toda tu informacion mediante un perfil de facebook

10. Qué elementos agregarías al tour virtual?(16 respuestas)

QUE SE PUEDA INTERACTUAR EN ELLA,

juegos para implementar lo aprendido controles de para audio

mas facilidad en la ruta para el ingresos al contenido

la verdad me gustaria investigar mas para dar este aporte, pero en si ubiera sido recomendable dar recomendaciones sobre que programas y antivirus son mejores y aceptables para aplicarlo

spams. mas tipos de phishin. hakeo.

Un juego como por ejemplo ahorcado o quien quiere ser millonario, que dinamice los temas y por ejemplo se tengan que adivinar los diferentes términos.

yo agregaria preguntas y respuestas dinamicas acerca de los videos que me dieran cierto puntaje por responderlas

agregar juegos relacionados con el aprendizaje

profundizar en como o a quien acudir, tipos de virus y potenciales peligros para los usuarios

actividades didácticas tales como juegos o competencias

avatar personalizado, mas salas con diferentes tematicas de aprendizaje y cultura general

N/A

Preguntas interactivas

La posibilidad de pausar los vídeos

tipos de virus, hacking, craking

otro avatar con el que puede interactuar el usuario a manera de dialogo sería una buena practica e implementacion para motivar a los usuarios

Anexo 8: Grabación incorporada en el diario de campo.

Inv. Qué pueden comentarme acerca de la actividad ¿cómo les pareció?

Est. Muy agradable, interesante, Dinámica, interactiva. Hace que uno le ponga más empeño a la clase, se parece a un videojuego

Inv. ¿Les llama la atención de que se parezca a un videojuego?

Est. Sí claro. Porque cambia la cátedra de dictar la clase en el tablero. Si tuviera pistola sería mucho mejor... (Risas)

Inv. Es un tour virtual en cambio de un videojuego, la idea era convertirlo en un videojuego pero tiene un trasfondo: diseño de personajes, guión, etc., por eso se maneja como un tour virtual. Buen aporte.

Inv. ¿En algún momento se sintieron cansados o les pareció monótono?

Est. Al final al observar los videos de TED...uno se concentra tanto que llega a un punto que se dispersa, a esta hora es complicado.

Inv. ¿Las presentaciones cómo les parecieron?

Est. Muy didácticas, enfocadas para los jóvenes.

Inv. ¿Qué es sexting?

Est. Cuando alguien publica fotos íntimas.

Inv. ¿Qué es grooming?

Est. Son por ejemplo, los abusos sexuales que hacen los acosadores por medio de redes haciéndose pasar por adolescentes.

Inv. Hablando de ataques informáticos, ¿Qué son lo hoax?

Est. Son mensajes que buscan obtener información

Inv. Es cierto, por ejemplo cuando llega un correo diciendo que Bill Gates está repartiendo su fortuna y el usuario comparte sus datos personales.

Inv. Y el Phishing, ¿Qué es?

Est. Suplantación de una página web para sacar datos de autenticación.

Inv. Un ejemplo es el caso de Davivienda que produjo pérdidas considerables a la compañía, ocasionadas porque las personas estaban sacando masivamente sus dineros de esta entidad por un rumor a partir de un hoax. Aunque los bancos tienen medidas preventivas como el encaje bancario.

Inv. ¿Qué recomendaciones les brindó el tour virtual ante este ataque?

Est. Digitar uno mismo la url de las entidades bancarias no por enlace, verificar que tenga el protocolo https.

Inv. ¿Y qué es spoofing?

Est. Existe Spoofing de varios tipos IP Spoofing, El atacante suplanta la dirección ip de la víctima. DNS Spoofing.

Inv. ¿Recuerdan qué recomendaciones se planteaban en el tour virtual para evitar este ataque?

Est. Utilizar el protocolo IPsec y las ACL.

Inv. ¿Recuerdan qué son las ACL?, concepto visto en la asignatura de redes

Inv. Son las Listas de Control de Acceso, que se configuran en el Router, para permitir o denegar rangos de direcciones IP.

Anexo 9: Formato de Autorización.

FORMATO DE AUTORIZACIÓN

“Influencia en el aprendizaje de un Mundo Virtual Relativo a Conceptos Básicos de Seguridad Informática”

Estimado Estudiante:

El proyecto de investigación del título anterior, adscrito al Centro de Tecnologías para la Academia de la Universidad de La Sabana, se implementará a partir de un material educativo elaborado con la herramienta 3d Unity.

El proyecto tiene como propósito:

- ✓ Identificar riesgos en las redes sociales (grooming y sexting)
- ✓ Examinar las competencias acerca de los ataques informáticos: Hoax, Phishing y Spoofing.
- ✓ Reconocer algunas buenas prácticas para minimizar los riesgos en las redes sociales y los ataques informáticos.

Además, examinar la incidencia del tour virtual como propuesta pedagógica en el aprendizaje de los conceptos mencionados. También se pretende examinar las interacciones que se generan entre usted, sus compañeros, su docente y el material educativo.

Para el cumplimiento de estos objetivos recogeremos datos por medio de observaciones recopiladas con grabaciones en audio, fotografías, cuestionarios y entrevistas durante el desarrollo de la clase.

Su participación es de vital importancia en este proyecto y es de carácter voluntario. Si usted así lo define, puede desistir de participar y no se cuestionará su decisión. Se le garantiza:

- ✓ El uso anónimo para identificar las entrevistas y los cuestionarios.
- ✓ La oportunidad de verificar las declaraciones hechas en las entrevistas y la interpretación que se haga de ellas
- ✓ Que se le responderá cualquier duda que le genere el proyecto

Agradecemos de antemano su autorización para contar con usted como participante en este proyecto.

Cordialmente,

Juan Camilo Gutiérrez Pinzón
Investigador

Nombre _____
Firma: _____
C.C. _____