universidad cenfotec_
tecnologías de información y comunicación

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Elaboración de un curso introductorio en ciberseguridad orientado a padres de familia y tutores de menores de edad en general

Autor:

Ramírez Salazar Leonardo

Enero de 2021

Dedicatoria

A mi padre y a mi madre, a quienes les debo todo lo que soy.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Leonardo Ramírez Salazar.**

MIGUEL PEREZ MONTERO (FIRMA)

M. Sc. Miguel Pérez Montero
Tutor

M. Sc. Roberto Monje Aguilar
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)

Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2021.03.08 16:46:42 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 05 de marzo de 2021

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de Contenidos

Resumen

Para esta investigación se ha elaborado un curso de carácter introductorio en ciberseguridad orientado a padres de familia y tutores de menores de edad en general, que permita desarrollar en el hogar una cultura de ciberseguridad como parte de la vida diaria. Con este se procura crear conciencia sobre los peligros que el mundo digital conlleva, así como la explicación de buenas prácticas y manejo seguro de los datos personales sensibles de los menores de edad.

Actualmente, los menores de edad se enfrentan a muchas de las amenazas que la era digital trae, peligros tanto de índole técnico (manejo de contraseñas, conexión segura a redes públicas, malware, etc.) como de índole social (ingeniería social, *ciberbullying*, *sexting*, *grooming*, etc.).

Lamentablemente no se están realizando muchos esfuerzos en la creación de una cultura de seguridad de la información como demuestra el dramático aumento de ciberdelitos en el mundo, que van desde estafas hasta trata de persona. Aunque en Costa Rica las instituciones públicas, como el Ministerio de Ciencia y Tecnología (MICITT) o el Ministerio de Educación Pública (MEP), han lanzado campañas de concienciación sobre la importancia de la ciberseguridad, todavía no se ha cristalizado este acervo en un programa formal que incluya los aspectos más importantes de la seguridad de la información —desde los técnicos hasta los sociales—, así como metodologías para aplicarlos de manera efectiva en las aulas o en el entorno familiar.

Este trabajo busca dar un primer paso en una futura familia de productos y materiales educativos en materia de ciberseguridad que brinden aportes al currículo y formación de las nuevas generaciones, las cuales estarán cada vez más inmersas en la era digital y necesitarán poseer una sólida formación en la seguridad de la información para los desafíos que afrontarán.

Cabe destacar también que, si bien el objetivo de este trabajo está orientado a personas que tienen a su cuidado menores de edad, la mayoría de los temas que se tratarán son aprovechables y útiles para personas de toda edad y condición, pues los peligros y la protección de los datos personales son aspectos que afectan a cualquier miembro de la sociedad.

Palabras clave: ciberseguridad, *ciberbullying*, cultura de la ciberseguridad, menores de edad, ciberacoso, *grooming*, *sexting*, *sharenting*, seguridad de la información.

Capítulo 1. Introducción

1.1 Generalidades

Debido a los cambios sociales generados el año 2020 debido a la pandemia mundial de Covid-19, se decidió elaborar el curso en modalidad virtual, diseñándolo para ser o bien, ofrecido a una institución como universidad Cenfotec como parte de sus cursos libres en línea o bien, para ser publicado en una plataforma virtual educativa de manera gratuita y al alcance de la ciudadanía.

1.2 Antecedentes del Problema

Este trabajo aporta un curso introductorio a la ciberseguridad que busca informar y crear conciencia en padres de familia y tutores (PyT) de menores de edad sobre los peligros y amenazas que el mundo digital conlleva, así como la prevención de las mismas. Su propósito es dar un valor añadido que enriquezca su formación en un aspecto tan necesario en la actualidad como la seguridad de la información.

Preliminarmente no se han logrado identificar instituciones a nivel nacional que tengan algún curso o capacitación en ciberseguridad establecido. Es poco probable que esto esté implementado o tan siquiera pensado en la mayoría de instituciones privadas y mucho menos en las públicas, si se toma en cuenta que este tema es una materia pendiente y en discusión en países más desarrollados en lo tecnológico. Ciertamente a nivel estatal se han realizado tímidos esfuerzos sobre este particular, tales como campañas de concientización en forma de infografías o charlas ocasionales, pero no existe un curso que introduzca a los PyT en la ciberseguridad para trabajar estos temas con menores de edad como parte de la vida cotidiana.

En Costa Rica, en el año 2019 se publicó la primera encuesta nacional sobre el uso de la tecnología móvil y violencia en línea en menores de edad (Paniamor, 2019), por lo que desde hace muy poco se están realizando sondeos formales sobre la situación actual de los menores y las tecnologías de la información.

1.3 Definición y descripción del problema

El problema consiste en las crecientes amenazas y peligros a los que los menores de edad se enfrentan en la actualidad a la hora de utilizar tecnologías de la información; amenazas tanto técnicas (*malware*, conexión segura a redes, manejo de contraseñas, etc.) como sociales (*ciberbullying*, *sexting*, *grooming* entre otras), así como el desconocimiento en la gestión de datos personales y sensibles.

Si bien los delitos informáticos no son una actividad nueva y tienen una larga data, con la progresiva democratización de Internet y un mayor acceso a los productos y servicios desde la red, el cibercrimen se ha disparado gracias a este uso masivo de las tecnologías de la información. Como muestran las crecientes cifras de cibercrimen, dada por organismos nacionales e internacionales, la ciudadanía no está lo suficientemente informada o preparada para prevenir y evitar ser víctimas de estas nuevas formas de delitos. Esto no siempre ocurre por desidia, ya que al vivir en un mundo tecnológico que evoluciona y cambia a gran velocidad es difícil que una persona no especializada esté al tanto de cómo las ciberamenazas aparecen y evolucionan, pues tiene otras responsabilidades y ocupaciones.

Con la pandemia de COVID-19 esas amenazas se han agravado, pues se ha medido un dramático aumento del cibercrimen en todo el mundo debido a las medidas de aislamiento y burbujas sociales que han generado un mayor consumo de productos y servicios por Internet y un mayor tiempo de exposición en línea. De esta situación los cibercriminales se han aprovechado para expandir sus actividades delictivas. Es de esperar que será difícil volver a la como era antes; la llamada nueva normalidad llegó para quedarse, y con ella todo este tipo de amenazas crecientes. Asimismo, puede que en el futuro próximo existan nuevas pandemias o situaciones que potencien esta nueva realidad.

Avanzamos hacia un mundo incierto y complejo que requerirá de la mejor preparación como ciudadanos para sacar a nuestro país adelante.

1.4 Justificación

La clave del desarrollo de la sociedad en nuestra era radica en el capital humano y en qué tan preparadas estén las nuevas generaciones para afrontar los nuevos retos que se avecinan gracias a las tecnologías de la información en áreas tan revolucionarias como la inteligencia artificial, la robótica, la realidad aumentada o la automatización de procesos. Estas áreas revolucionarán actividades de todo tipo, desde la medicina hasta el periodismo o la educación.

Uno de los temas claves de este nuevo mundo digital es el conocimiento sobre cómo resguardar, manipular y dar un uso adecuado a la información personal. Por abrir un correo electrónico las personas pueden perder toda la información de su dispositivo, terminar con sus cuentas de ahorro vacías, o perder su trabajo por hacer un comentario o publicar una foto fuera de lugar en una red social. En otras palabras, el tema de una cultura de la ciberseguridad para la ciudadanía es prioritaria y la justificación principal por la que se ha decidido realizar este trabajo

es debido a un concepto que durante toda la formación académica en ciberseguridad del autor de este trabajo, se menciona y enfatiza reiteradamente: “El eslabón más débil de la cadena en términos de ciberseguridad es el ser humano”, refiriéndose al hecho de que la mayoría de ciberdelitos se originan no por fallas de índole técnico, sino por errores de las personas a la hora de gestionar la información.

Por lo tanto, es de gran importancia el desarrollo de una cultura de la seguridad de la información para la ciudadanía en general, pues cuanto más educación y conciencia exista en estos temas, se reducen las oportunidades que los ciberdelincuentes puedan aprovechar.

Como todo hábito, empezar este proceso formativo desde edades tempranas y desde la familia es esencial y solo puede llevarse a cabo si los PyT están debidamente informados e instruidos en temas de ciberseguridad. Así podrán servir de guías a los niños y adolescentes en el uso adecuado de las tecnologías de la información, no solo como mentores, sino también dando el ejemplo con sus acciones, pues el cibercrimen afecta a todos.

Con la elaboración de este curso se ha buscado producir contenidos que sean de utilidad para PyT con inquietudes, dudas o pocos conocimientos sobre el uso adecuado de las tecnologías de la información por parte de sus hijos, generando así un valor agregado que aporte beneficios a la sociedad.

1.5 Objetivos

Para este TFG se emplea la taxonomía de Bloom revisada; esto debido a que para una investigación aplicada resulta muy intuitiva para organizar la secuencia de pasos de la investigación, es robusta y el uso de verbos va más acorde con una investigación que busca resolver un problema.

Finalmente, este tipo de jerarquía es la más utilizada en trabajos de investigación en el país, lo cual facilita el acceso y comprensión rápida por parte de la comunidad.

1.5.1 Objetivo General

Elaboración de un curso introductorio en ciberseguridad orientado a padres de familia y tutores de menores de edad.

1.5.2 Objetivos Específicos

1) Identificar las ciberamenazas a las que los menores de edad están expuestos actualmente.

2) Comprender las ciberamenazas identificadas, sus características, posible impacto, manejo y prevención.
3) Escoger los temas, metodologías, materiales y contenidos que se implementarán para el curso.
4) Investigar los temas a desarrollar en el curso.

1.6 Alcances y Limitaciones

1.6.1 Alcances

Se ha elaborado un curso virtual constituido por una serie de videos para cada sesión; mediante el uso de presentaciones se abarcan los diferentes temas a tratar. Adicionalmente se adjunta un archivo de anexos donde se incluyen enlaces a materiales didácticos e información complementaria del curso.

1.6.2 Limitaciones

Debido a todas las dificultades con las que las instituciones educativas y padres de familia han tenido que lidiar para adaptarse a las nuevas normativas que la pandemia de COVID-19 ha impuesto, se decidió no aplicar el curso a una población pues se volvió muy difícil lograr una muestra significativa en un corto período de tiempo. Lo anterior, porque para ello sería necesario la coordinación con alguna institución y la anuencia de los padres de familia a realizarlo, algo complejo dado que las prioridades de las personas e instituciones son otras en la situación actual.

1.7 Estado de la cuestión

1.7.1 Planificación de la revisión

En esta etapa se identifica la necesidad de la revisión y se indica cuáles son sus objetivos, qué fuentes se utilizan para identificar los estudios primarios, si hubo algunas restricciones, cuáles son los criterios de inclusión y exclusión, qué criterios se utilizan para evaluar la calidad de los estudios primarios y cómo se extraen y sintetizan los datos de los estudios.

1.7.1.1 Pregunta de investigación

¿Qué trabajos e investigaciones aplicadas a la educación en ciberseguridad se han llevado a cabo orientadas a los menores de edad?

1.7.1.2 Palabras clave y sinónimos

Ciberseguridad, Escuelas, Menores de edad, Cuidado parental.

1.7.1.3 Intervención

En el contexto de la revisión sistemática se observan las propuestas existentes sobre la ciberseguridad aplicada a la educación de menores de edad, se obtienen los documentos más importantes y se procede a un posterior análisis de los mismos.

1.7.1.4 Resultado

Los resultados esperados de esta revisión son conocer las propuestas existentes en cuanto a la educación en ciberseguridad para menores de edad, analizarlas y conocer qué comparten y en qué difieren, además de identificar necesidades de investigación al encontrar puntos no tratados o profundizados.

1.7.1.5 Aplicación

Los beneficiarios de la revisión sistemática son las personas (académicos, investigadores, profesionales en ciberseguridad, profesores, padres de familia, tutores legales, etc.) relacionadas con la seguridad de la información como parte del proceso educativo y de formación en menores de edad.

1.7.1.6 Diseño experimental

El meta-análisis de la revisión está enfocado en la información disponible sobre la ciberseguridad aplicada en menores de edad presentes en los estudios primarios, para conocer las tendencias actuales según el área o áreas de interés en las que se centran.

1.7.2 Selección de fuentes

En este apartado se analiza principalmente la fuente que se usa para realizar la ejecución de la revisión. Posteriormente se utilizan los elementos definidos en la planificación para aplicar el procedimiento de obtención de estudios primarios en cada una de las fuentes seleccionadas.

1.7.2.1 Definición del criterio de selección de fuentes

El criterio para la selección de las fuentes de búsqueda está basado en una investigación previa del autor sobre ventajas y facilidades de ciertas fuentes sobre otras utilizando como requisitos el acceso vía web, motores de búsqueda que permiten consultas avanzadas, la amplitud de repositorios consultados y, finalmente, una cuestión de limitaciones financieras, pues muchos repositorios son de pago.

1.7.2.2 Fuente seleccionada

La fuente seleccionada para la revisión es Google Scholar, la cual maneja un completo motor de búsqueda avanzado. Además, permite el acceso a todo tipo de documentos tales como artículos, tesis, trabajos finales, libros y de diferentes repositorios. Al incluir material de repositorios institucionales se tiene acceso a las versiones web de texto completo de algunos artículos que las bases de datos no tienden a enlazar. También se trata de una herramienta gratuita que, si bien lo que hace es indexar resultados de diferentes fuentes y muchas de estas pueden llevar a sitios de pago, por experiencias anteriores con su manejo, la mayoría de veces se trata de información gratuita.

1.7.2.3 Cadenas de búsqueda

Utilizando operadores AND sobre las palabras clave y conceptos relacionados que se han identificado anteriormente, se pasa a establecer la cadena de búsqueda a utilizar en la presente revisión:

Ciberseguridad AND Escuelas AND Educación AND Cuidado parental.

1.7.3 Selección de los estudios

Una vez que se ha seleccionado la fuente, es necesario describir el proceso y el criterio que se va a seguir para ejecutar la revisión, selección y evaluación de los estudios primarios. Para ello se define el proceso completo de selección, así como los criterios de inclusión y exclusión tomados en cuenta.

En esta revisión se hará un proceso iterativo e incremental, conformado por las etapas de búsqueda, extracción y visualización de la información de la fuente seleccionada. En primer lugar, se adapta la cadena a la fuente seleccionada y se ejecuta la consulta. Sobre el conjunto de resultados obtenidos se aplica el criterio de inclusión a modo de filtro, de forma que obtengamos un conjunto de estudios relevantes. A continuación, sobre este conjunto de estudios relevantes se aplica el criterio de exclusión, para obtener el conjunto de estudios primarios, los cuales pasamos a almacenar y a analizar en más profundidad extrayendo su información bibliográfica y la información relevante de cada uno de ellos en base a un formulario previamente definido.

1.7.3.1 Definición del criterio de inclusión y exclusión de estudios

El criterio de inclusión actúa sobre los resultados obtenidos al ejecutar la búsqueda sobre la fuente, permitiendo realizar una primera selección de documentos que son considerados en el contexto de la revisión como candidatos a convertirse en estudios primarios.

Como criterio de inclusión se realiza principalmente un análisis sobre el título, las palabras claves y el resumen de cada documento, de esta forma se puede ver en una primera vista cómo están relacionadas estas palabras y por qué ha sido seleccionado dicho documento. Con este criterio se eliminan la mayor parte de los resultados obtenidos que no dan aportes sobre la pregunta de investigación planteada.

El criterio de exclusión actúa sobre el subconjunto de documentos obtenidos en la etapa anterior y permite obtener el conjunto de estudios primarios. El criterio de exclusión se centra principalmente en la lectura y análisis del resumen del documento y sus conclusiones, teniendo en algunos casos que profundizar en el mismo. Con este criterio se puede ver en más detalle de qué trata cada documento, ver la relación real que presenta con los objetivos buscados y si es verdaderamente relevante para la revisión, seleccionándolo como estudio primario.

1.7.3.2 Definición de tipos de estudio

Los tipos de estudios primarios que son seleccionados durante la ejecución de la revisión sistemática son los artículos presentes en las fuentes seleccionadas que cumplan con los criterios establecidos.

1.7.4 Ejecución de la revisión

En esta sección se aplica la revisión a Scholar Google, para obtener nuevos estudios primarios.

1.7.4.1 Selección de estudios iniciales

Al utilizar la consulta inicial en el motor de búsqueda se obtuvieron resultados escuetos. Por lo tanto, se procedió a utilizar como palabras clave los términos “ciberseguridad” y “escuelas” y se obtuvieron 800 resultados, de los cuales se revisaron los primeros 100. Tras aplicar el criterio de inclusión, se seleccionaron 21 criterios relevantes, y seguidamente se aplicó el criterio de exclusión y se obtuvieron 10 estudios primarios:

01	Astorga, C. y Schmidt, I. (Setiembre-diciembre 2019). “Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad”. *Revista electrónica Educare*. Vol 23(3), pp.1-24. Recuperado de: enlace
02	PROSIC. (2010). Ciberseguridad en Costa Rica. Recuperado de: enlace
03	Giant, N. (2016). Ciberseguridad para la i-generación. Recuperado de: enlace
04	Cuesta, F.; Rico, D.; Anderson, C.; Portillo, E.; Sánchez, L.; Vera, M.; Alvernia, S.; Rueda, J.; Sánchez, T.; Sánchez, B.; Bacca, R. y Cantillo, A. (2016). Inseguridad en las redes sociales e Internet: prioridad en las escuelas de la provincia Ocaña. Recuperado de: enlace
05	Guerrero, D.; Moncayo, L. y Parra, J. (2015). Cyberbullying, el acoso escolar en la era virtual. (Tesis de grado). Instituto Alberto Merani. Recuperado de: enlace
06	Davara, L. (enero-abril 2019). Formación TIC (redes sociales, internet, ciberseguridad, *big data*, etc.) en casa, en el colegio, en la universidad y en las empresas: características, razón de ser y contenido. CEF, num12, pp.89-110. Recuperado de: enlace
07	Martínez, G. (2018). La Mediación Parental en Internet: estrategias, prevalencia y eficacia en Europa y en España. (Tesis doctoral). Universidad del País Vasco. Recuperado de: enlace
08	Porcar, S. (2018). La protección de la privacidad de los menores en internet. (Tesis de grado). Universitat Jaume 1. Recuperado de: enlace
09	Sofía, C. (2018). Seguridad en los niños mediante herramientas de control parental que permita a los padres supervisar el uso de Internet. Informe de proyecto de maestría. Instituto politécnico de Leiria. Recuperado de: enlace
10	García, J. (2017). Seguridad y riesgos: *Ciberbullying*, *Grooming* y *Sexting*. (Trabajo final de maestría). Universidad Autónoma de Barcelona. Recuperado de: enlace

1.7.4.2 Evaluación de la calidad de los estudios

Todos los documentos presentes en la fuente Google Scholar tienen presunción de calidad, ya que para estar indexados en este buscador han debido pasar por una serie de filtros y evaluaciones.

1.7.4.3 Extracción de la información

En esta sección se realiza el análisis de la información relevante de cada uno de los estudios primarios que se han obtenido en los pasos anteriores.

1.7.4.3.1 Formulario para la extracción de la información

El formulario consta de una primera parte de identificación del estudio en la que muestra el título, publicación y autores del documento. La segunda parte se compone de la descripción general en la que se presenta un breve resumen y el área de interés que aporta datos. Finalmente, hay una sección donde se presentan aspectos a destacar para el desarrollo de la investigación.

1.7.4.3.2 Extracción de resultados objetivos y subjetivos

Identificación
Título: Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad.
Publicación: (Setiembre-diciembre 2019) Revista electrónica Educare. Vol 23(3), pp.1-24
Autores: Astorga, C. Schmidt, I.
Descripción
Área: Investigación y Docencia en educación
Resumen: Análisis del estado del arte en Costa Rica sobre el nivel de alfabetización en el uso de redes sociales y la protección por medio de buenas prácticas de los menores de edad.
Aspectos a destacar
• Se trata la brecha generacional como un problema para los padres de familia y educadores. • Se presentan las actividades predilectas que practican los menores de edad en Internet. • Se presentan las redes sociales más usadas por menores de edad en Costa Rica. • Se mencionan los riesgos principales a los que los menores de edad están expuestos ante las redes sociales. • Se apunta a los padres de familia como la principal barrera de defensa contra el cibercrimen en la familia. Se ofrecen soluciones y técnicas para educar en ciberseguridad a los niños en el hogar.

- Proporciona una visión general y actual del estado de la ciberseguridad en los hogares costarricenses.

Identificación
Título: Ciberseguridad en Costa Rica
Publicación: PROSIC. Universidad de Costa Rica
Autores: PROSIC
Descripción
Área: Ciberseguridad en el ámbito nacional
Resumen: 16 ponencias realizadas en la UCR para examinar el impacto de las nuevas tecnologías en la sociedad costarricense en este caso en la ciberseguridad.
Aspectos a destacar
• Amplia documentación sobre aspectos jurídicos de la protección y manejo de datos en Costa Rica. • Pautas detalladas para proteger la información en el hogar.

Identificación
Título: Ciberseguridad para la i-generación
Publicación: Publicaciones narcea. 2016.
Autores: Giant, N.
Descripción
Área: Alfabetización y gestión en ciberseguridad
Resumen: Libro que expone los riesgos, plantea soluciones y propone diferentes estrategias para la ciberseguridad en el hogar y las aulas desde un enfoque integral entre el hogar y el centro educativo.
Aspectos a destacar
• Presenta procedimientos para la creación de una cultura holística en torno a la ciberseguridad en la escuela y la familia. • Presenta procedimientos para la creación de un plan de respuesta a incidentes ante la aparición de uno en la seguridad de la información.

- Expone temas de gran importancia tales como la creación de normativas y políticas institucionales y plantillas para realizar una encuesta de aproximación al ecosistema de maestros-estudiantes-padres y sus conocimientos y hábitos en la red.

Identificación
Título: Inseguridad en las redes sociales e Internet: prioridad en las escuelas de la provincia Ocaña
Publicación: Fondo Editorial ITM (2016).
Autores: Cuesta, F.; Rico, D.; Anderson, C.; Portillo, E.; Sánchez, L.; Vera, M.; Alvernia, S.; Rueda, J.; Sánchez, T.; Sánchez, B.; Bacca, R. y Cantillo, A.
Descripción
Área: Ciberseguridad aplicada en escuelas
Resumen: El libro muestra un caso de aplicación de estrategias en ciberseguridad aplicadas a las escuelas de primaria de la provincia de Ocaña en España.
Aspectos a destacar
• Primer documento que indica un rango de edad para iniciar la educación de los niños en ciberseguridad. En este caso edades entre los 9-10 años. Este dato puede ser comparado con información suministrada por la institución a trabajar en esta investigación para fijar el rango en el país o mantener el mismo. • Presentación de las etapas y planificación del plan para implantar el programa de alfabetización de ciberseguridad.

Identificación
Título: Cyberbullying, el acoso escolar en la era virtual
Publicación: Instituto Alberto Merani (2015)
Autores: Guerrero, D.; Moncayo, L.; Parra, J.
Descripción
Área: Educación
Resumen: Estudio colombiano sobre el impacto del *cyberbullying* en diferentes edades y estratos sociales, así como sus causas, tipos y problemas que acarrean en la sociedad actual.
Aspectos a destacar

- Presenta un estudio estadístico de cómo actúa el *cyberbullying*, así como una descripción minuciosa de esta actividad de la red. Al ser una muestra de un país latinoamericano tan cercano culturalmente a Costa Rica, puede ser de utilidad para establecer algunas semejanzas.

Identificación
Título: Formación TIC (redes sociales, internet, ciberseguridad, *big data*, etc.) en casa, en el colegio, en la universidad y en las empresas: características, razón de ser y contenido
Publicación: CEF, num12, pp.89-110 (enero-abril 2019)
Autores: Davara, L.
Descripción
Área: Alfabetización digital en ciberseguridad.
Resumen: Justificación de la importancia de la implantación de una cultura en ciberseguridad integral a lo largo de las diferentes edades y etapas de vida.
Aspectos a destacar

- Presenta un modelo de alfabetización comenzando con la educación primaria y terminando con la vida laboral.
- Presenta la necesidad de ver a la ciberseguridad como una asignatura más en el plan de estudios institucionales primario, secundario y superior.
- Se da un enfoque de alfabetización a nivel de 4 categorías en la sociedad: menores de edad, padres, estudiantes y profesionales mayores de edad y profesores.
- Maneja una alta segmentación para menores de edad y diferentes estrategias de ciberseguridad para cada segmento.

Identificación
Título: La Mediación Parental en Internet: estrategias, prevalencia y eficacia en Europa y en España
Publicación: Universidad del País Vasco (2018)
Autores: Martínez, G.
Descripción
Área: Alfabetización en ciberseguridad

Resumen: Compendio de diferentes artículos dirigidos a las medidas y el papel a tomar por los padres de familia en la educación en ciberseguridad de sus hijos desde el marco de desarrollo de la red europea EU Kids Online.
Aspectos a destacar
• Manejo y gestión de riesgos en el uso de Internet. • Análisis minucioso de la mediación parental: estrategias, predicciones, gestión, efectividad, etc.

Identificación
Título: La protección de la privacidad de los menores en internet
Publicación: Universitat Jaume 1. (2018)
Autores: Porcar, S.
Descripción
Área: Aspectos éticos y legales
Resumen: Análisis de la situación legal de los derechos y la protección de datos de los menores de edad en España.
Aspectos a destacar
• Analiza diferentes mecanismos de protección de la privacidad en internet. • ¡Importante! Tiene una sección completa donde analiza la injerencia de los padres en la intimidad de los menores.

Identificación
Título: Seguridad en los niños mediante herramientas de control parental que permita a los padres supervisar el uso de internet
Publicación: Instituto politécnico de Leiria
Autor: Sofía, C. (2018)
Descripción
Área: Alfabetización en ciberseguridad
Resumen: Se propone una capacitación que ayude a los padres de familia a aumentar su nivel de conocimiento de herramientas de control parental para disminuir los riesgos a los que están expuestos los estudiantes de un centro educativo.
Aspectos a destacar

• Este artículo aborda la ciberseguridad desde un enfoque técnico en la capacitación de padres de familia en el uso de herramientas tecnológicas, un factor que he extrañado mucho en los otros documentos de esta revisión pues muestra algunos productos de *software* de control parental líderes del mercado y su empleo.

Identificación
Título: Seguridad y riesgos: *Ciberbullying*, *Grooming* y *Sexting*.
Publicación: Universidad Autónoma de Barcelona (2017).
Autores: García, J.
Descripción
Área: Alfabetización en ciberseguridad
Resumen: La investigación busca definir a profundidad los conceptos de *Cyberbullying*, *Grooming* y *Sexting*, principales, víctimas, consecuencias y recomendaciones para su prevención.
Aspectos a destacar
• Es una investigación complementaria para los artículos principales de esta revisión.

1.7.5 Resultados

Todos los documentos elegidos afrontan el problema de la educación en ciberseguridad desde puntos de vista diferentes, enriqueciendo grandemente el conjunto de conocimientos y mostrando en todos ellos la importancia de generar una cultura de la ciberseguridad desde edades tempranas. Se encontraron:

- Artículos con un fuerte énfasis en redes sociales y las amenazas que estas pueden generar de no manejarse de manera correcta, tales como el *ciberbullying*, el *sexting* o el *grooming*.
- Documentos con un énfasis centrado en cuestiones del ámbito legal y ético sobre la protección y manejo de datos privados.
- Artículos que ilustran de manera teórica y aplicada la creación de capacitaciones en la enseñanza de la ciberseguridad para personas a cargo de menores de edad.
- Artículos centrados en la presentación y aprendizaje de herramientas de software de cuidado parental.

- Además, se establece el ciberacoso como una de las amenazas más recurrentes y preocupantes a las que se enfrentan los menores.
- Finalmente, se establece a los padres de familia como los actores principales en la educación de los menores de edad en temas de ciberseguridad.

Sin embargo, la revisión bibliográfica también arrojó algunas deficiencias en el desarrollo de ciertos temas que se consideran de importancia. Se pueden citar en este grupo los juegos en línea multijugador donde los menores de edad pueden exponerse a amenazas también de tipo *grooming* o de *malware* que puede infectar los dispositivos de su red local. Además, si bien se halló información técnica sobre el uso de programas de control y cuidado parental, no se encontraron buenas prácticas y medidas básicas para la protección de la información, tales como accesos seguros a redes públicas o la importancia de la privacidad y fortalecimiento en las contraseñas de acceso.

Un aspecto que llama la atención es que la mayoría de documentos están elaborados por profesionales en el campo de la educación y abordan temas de ciberseguridad, pero pocos desde el lado de tecnologías de información, con lo cual la parte relacionada con aspectos éticos y sociales está muy reforzada. Hay una importante cantidad de documentación relacionada con peligros de las redes sociales, *sexting*, *grooming*, *ciberbullying*, etc. Sin embargo, hay deficiencias a nivel de educación sobre amenazas a nivel técnico, tales como acceso seguro a redes, *malware*, etc.

Capítulo 2. Marco teórico conceptual

Dado que esta investigación es de tipo aplicado, se requiere la evaluación de un marco conceptual para la aclaración de algunos conceptos claves. Para ello, se genera una nube de palabras y con base en esta un mapa conceptual con las definiciones de los términos encontrados.

2.1 Nube de palabras conceptual

Para crear la nube de palabras se utiliza la herramienta *Tag Crowd*. Se selecciona el idioma español y se copia la información obtenida del estado de la cuestión; se eliminan los artículos, pronombres y conjunciones.

La nube resultante se presenta en la figura 1:

Figura 1 Nube de palabras conceptual.

Fuente: confeccionado por el autor a partir del estado de la cuestión

2.2 Mapa conceptual jerárquico

Para este mapa conceptual solo algunas palabras serán definidas. El criterio empleado por el autor se establece en lo singular que sea el término dentro del contexto de la ciberseguridad.

El mapa conceptual se muestra en la figura 2:

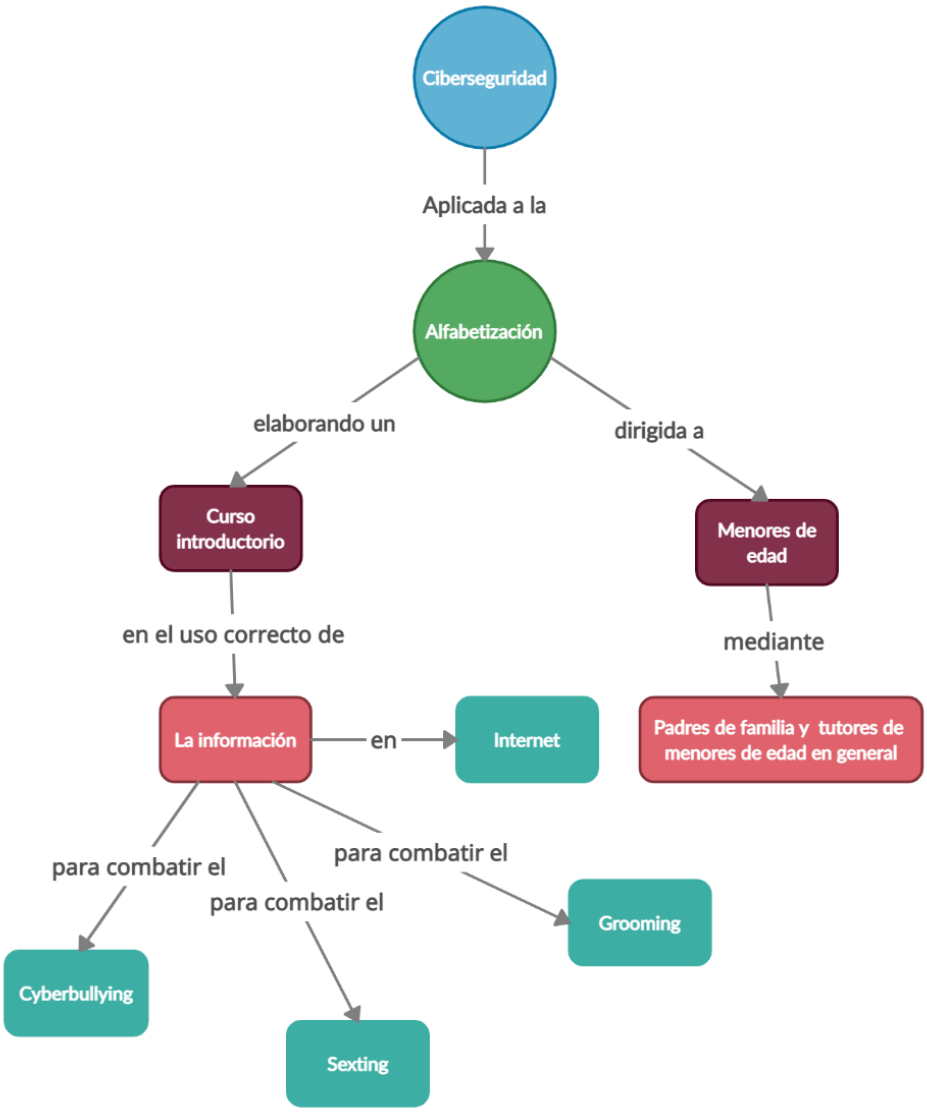

Figura 2. Mapa conceptual

2.3 Glosario

- **Ciudadanía digital**: Consiste en la participación ciudadana a través de las tecnologías de la información y comunicación en internet y las redes sociales. La ciudadanía digital incluye aspectos como normas de comportamiento en el mundo virtual, alfabetización digital, participación ciudadana, seguridad digital, etc.
- **Cultura de la seguridad de la información**: Es el conjunto de hábitos y buenas prácticas empleadas por las personas en la gestión y protección de la información. La cultura de la seguridad puede darse a nivel de organizaciones públicas y privadas o de manera individual a nivel de la ciudadanía.
- ***Cyberbullying*:** El *ciberbullying* es el acoso que tiene lugar en dispositivos digitales, como teléfonos celulares, computadoras y tabletas. El *ciberbullying* incluye enviar, publicar o compartir contenido negativo, perjudicial, falso o cruel sobre otra persona. Esto puede incluir compartir información personal o privada sobre alguien más, provocándole humillación o vergüenza. Algunos acosos por Internet pasan a ser un comportamiento ilegal o criminal.
- ***Deep Fakes***: Consiste en la manipulación de vídeos e imágenes digitales mediante avanzados algoritmos (*deep learning*) de inteligencia artificial que buscan suplantar rostros y sonidos del contenido auténtico buscando que la versión falsificada sea indistinguible de la original. Este tipo de engaños pretenden generar desinformación en la ciudadanía o causar un daño moral a particulares presentándolos en situaciones falsas.
- ***Deep web* y *Dark web***: La *deep web* se trata de los contenidos no indexados (aproximadamente el 90% de toda la información en Internet) en los buscadores de uso común. La mayoría de esta información no pertenece a actividades ilegales y consiste en páginas convencionales con protecciones de acceso, bases de datos financieras, científicas, almacenamiento privado, etc. El 0,1% de Internet corresponde a la *dark web* y se trata de contenidos intencionalmente ocultos y solo accesibles con navegadores especiales dado que son sitios altamente cifrados. Si bien mucha de la *dark web* se emplea para que activistas perseguidos de regímenes represores puedan desempeñar su actividad, también es lugar de refugio para actividades ilegales como tráfico de drogas, armas, trata de personas, etc.
- ***Grooming*:** Es la práctica mediante la cual los adultos se hacen pasar por menores en Internet o intentan establecer un contacto con niños y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente, al chantaje con fines sexuales.
- **Huella digital**: Se trata de un concepto que engloba toda la información que las personas dejan cuando utilizan Internet. La huella digital incluye metadatos (edad, sexo, localización,

idioma, sistema operativo del dispositivo) e información como comentarios, imágenes o videos sobre todas nuestras actividades en la red.

- **Identidad digital**: Consiste en el perfil digital de las personas construido a partir de la huella digital y que compone la imagen de los individuos en la red: datos personales, comentarios, gustos, amistades, preferencias, etc. A mayor información recolectada a través de la huella digital, más detallada y exacta es esta identidad y ella determina la reputación y la opinión que tiene el resto de ciudadanos sobre un individuo en concreto.
- **Ingeniería Social:** Es un conjunto de técnicas y habilidades cuyo propósito es manipular a las personas para que hagan lo que el que el ingeniero social desee. En el mundo de la ciberseguridad, la ingeniería social es empleada por los ciberdelincuentes para extraer de los usuarios datos sensibles tales como contraseñas de seguridad, infectar los equipos de la víctima con malware o que abran enlaces a sitios fraudulentos entre otros.
- **Inteligencia artificial**: Conjunto de tecnologías que buscan imitar la inteligencia humana en alguna área de conocimiento y cuyos objetivos van desde estudios en las ciencias cognitivas hasta el poder automatizar procesos o tareas realizadas por humanos, ya sea a nivel mental (sistemas expertos) o a nivel físico (robots).
- **Internet de las cosas**: Consiste en la conexión de todo tipo de objetos físicos a Internet para que estos, mediante sus sensores, puedan intercambiar información en la red con distintos servicios. La Internet de las cosas (IoT) permite la programación de dispositivos remotos (robot barredores, cámaras de seguridad), la gestión de recursos del hogar (refrigeradores y alacenas inteligentes) o el monitoreo de signos vitales y de salud (ropa inteligente).
- ***Software* de control parental**: Son distintos tipos de programas a ser instalados en los dispositivos de menores de edad para que los PyT puedan asegurarse del uso correcto de estos. Estos programas tienen funcionalidades tales como el bloqueo a sitios con contenidos inapropiados, límite de tiempo de uso por cada aplicación, restricción a la instalación de aplicaciones sin autorización, etc.
- ***Ransomware***: Familia de virus informáticos que buscan dañar el funcionamiento de los dispositivos y de la información almacenada que infectan, exigiendo un rescate económico.
- ***Sexting***: Se denomina *sexting* a la actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, ya sea utilizando aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación.
- ***Sharenting*:** Práctica que consiste en la publicación por parte de los PyT en la red de todo tipo de información sobre los menores de edad (bebés o niños muy pequeños) para

documentar sus primeros pasos, cumpleaños, anécdotas, etc. A pesar de parecer una actividad inofensiva, los PyT están manipulando información personal del menor sin su consentimiento. Dicha información empieza a definir su identidad digital incluso antes de que el menor lo desee, dejando la puerta abierta a futuro para que estos sean blanco de actividades de cibercrimen tales como la suplantación de identidad y fraudes.

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

La investigación para este trabajo final de graduación es de tipo aplicada, pues se utilizan conocimientos existentes para atender una necesidad de la sociedad en particular.

3.2 Alcance investigativo

Para este trabajo final de graduación se elige como alcance investigativo el exploratorio. Esto debido a que el autor de la investigación nunca ha realizado un trabajo investigativo sobre el tema de ciberseguridad; por lo tanto, es un campo de conocimiento no revisado y del que se tiene dudas.

3.3 Enfoque

El enfoque de este trabajo final de graduación es cualitativo debido a que se utiliza un método inductivo (de lo específico a lo general), se estudia la realidad de manera natural, interpretando los fenómenos observados.

3.4 Diseño

El diseño cualitativo a emplear es de tipo investigación-acción. En este diseño el investigador ayuda a transformar la realidad utilizando dos procesos: el conocer (investigar, estudiar, recopila información) y actuar (interpretar los datos y aplicarlos en la resolución de un problema), pues su finalidad es práctica. Además, el investigador no es neutral y busca estimular el cambio y la transformación social.

3.5 Sujetos y fuentes de información

Los sujetos y las fuentes de información de este estudio son expertos de instituciones relacionadas con la protección del menor.

3.6 Instrumentos de recolección de datos

Para la recolección de datos de los sujetos involucrados en el trabajo de investigación se emplean:

- **Entrevistas**: Dirigidas a expertos. La entrevista tiene la finalidad de obtener más información sobre el estado de la ciberseguridad en menores de edad en el contexto nacional.

3.7 Técnicas de análisis de información

Para analizar la información que se recopila durante la investigación se emplea el diagrama de Ishikawa (cola de pescado). Este sistema permite identificar los diferentes problemas a tratar durante el desarrollo del trabajo y agruparlos en colecciones de causa (espinas) -> efecto (cabeza). La figura 3 presenta la estructura básica de un diagrama de Ishikawa.

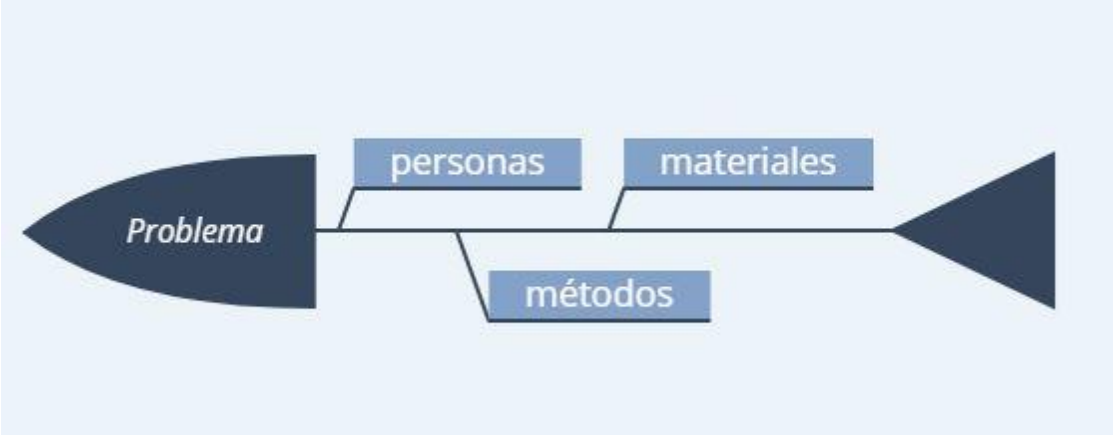

Figura 3. diagrama de Ishikawa.

Capítulo 4. Análisis de diagnóstico

Esta entrevista se estableció para tener una impresión actualizada de la situación en ciberseguridad del país. Se eligió la fundación Paniamor luego de investigar, en los distintos sitios gubernamentales y privados del país, qué actores están jugando un rol más activo en materia de ciberseguridad para menores de edad, lo cual dio como resultado que todos convergen en la fundación Paniamor como referente.

En una entrevista vía video llamada el 13 de marzo del 2020 con Mariam Carpio, gerente de proyectos sociales, especialista en comunicación y democratización del conocimiento y el cuidado de menores de edad de la Fundación, se obtuvo la siguiente información relevante:

1- Con la apertura de las telecomunicaciones en 2008 y la declaración del acceso a Internet en 2010 como un derecho fundamental, fundación Paniamor toma un papel activo en monitorizar cómo las tecnologías de la información afectan a los menores de edad. Funcionando como un actor que trabaja con instituciones públicas y privadas de manera transversal, como un observatorio que proporciona información sobre la situación de la niñez en Costa Rica. Cabe destacar que al no ser una institución pública y no tener ninguna afiliación política, esta no se ve sujeta a interferencias o interrupciones en sus proyectos debido a cambios de gobierno y o de ideologías políticas, y es un organismo consistente en su accionar.
2- En el año 2018 la fundación Paniamor desarrolló la primera encuesta nacional para entender los tipos de violencia y de mediación parental en Costa Rica, y sus resultados se publicaron en el año 2019. Este es un documento de gran valor, pues da la primera radiografía nacional sobre los hábitos y usos de las tecnologías de la información en los menores de edad y, por lo tanto, fue un material de consulta valioso a la hora de elaborar la solución de este trabajo.
3- La Fundación Paniamor -con apoyo de instituciones gubernamentales y organismos internacionales- ha desarrollado la primera plataforma digital para cuidado parental en tecnologías de la información llamada E-Mentores. Esta es referenciada tanto por el Patronato Nacional de la Infancia como por el Ministerio de Educación Pública
4- Se conocen los cuatro tipos de mediación parental identificados por la Fundación y empleados por los padres de familia a la hora de gestionar las tecnologías de la información con sus hijos: activa, activa negativa, restrictiva y permisiva.
5- Se brinda el dato de que las habilidades digitales de los cuidadores de menores están directamente relacionadas con las habilidades digitales de los menores de edad a su cargo. Con ello se confirma la premisa de que una correcta alfabetización a nivel de PyT es esencial en un buen desarrollo de una cultura de la ciberseguridad en los menores de edad.
6- Gracias a la encuesta nacional de usos de la tecnología móvil, la Fundación Paniamor ha llegado a la conclusión de que hay fuertes falencias en una correcta educación en ciberseguridad para los menores de edad, por lo cual hay mucho trabajo por hacer tanto desde el sector privado como público.

Capítulo 5. Propuesta de la Solución

En este capítulo se describe el diseño, procesos y herramientas de desarrollo de la solución propuesta. Se describen además los contenidos expuestos en cada sección de la solución.

5.1 Diseño de la solución

5.1.1 Diseño a nivel de forma y contenido

Este curso está pensado para padres de familia y cuidadores de menores de edad en general, con pocos o ningún conocimiento en materia de ciberseguridad. Por lo tanto, se trata de un curso de carácter introductorio cuyo propósito principal es, mediante un lenguaje amigable, formar y crear conciencia sobre las principales ciberamenazas que van aparejadas con las tecnologías de la información y comunicación (TICs) y que afectan a los menores de edad, así como el manejo preventivo y respuesta a incidentes de estas últimas.

Dado que la mayoría de estas amenazas afectan tanto a adultos como menores de edad (la ciberseguridad es un asunto de todos), se busca que todos los miembros de la familia se vean beneficiados con estos conocimientos, empezando a generar una cultura de la seguridad de la información en el hogar como meta principal.

El curso se ha elaborado bajo la modalidad de E-Learning asincrónico, aunque puede ser adaptado fácilmente a una modalidad sincrónica si esto fuese requerido a futuro por un grupo de personas o una entidad interesada en algo más participativo o personal. Esta decisión es debido a los requerimientos de las nuevas normas impuestas por la pandemia de COVID-19. Reunir a un grupo de padres de familia de manera presencial es impensable en la situación actual y una sesión sincrónica necesita de la disponibilidad de los interesados en una franja horaria común para todos. Algo difícil de realizar incluso con la ayuda del personal de una institución educativa, pues el año 2020 fue particularmente difícil tanto para alumnos como para profesores y PyT, quienes tuvieron que adaptarse a situaciones que generaron cargas laborales, nuevas modalidades de estudio y acumulación de estrés, por lo que las prioridades eran otras.

El año 2021 es más factible para aplicar un curso en modalidad asincrónica: las personas están más acostumbradas a las nuevas condiciones de la pandemia y un curso asincrónico

permite a cada participante llevarlo a su ritmo y en el horario que más le convenga. Es lo recomendable en la situación actual, cuando muchas familias disponen de pocos dispositivos conectados a Internet y estos deben de compartirse entre todos los miembros del hogar.

El curso tiene una duración de aproximadamente seis horas, ya que al ser una introducción a la ciberseguridad para principiantes, se buscó abarcar la mayor cantidad de contenidos importantes de una manera general y en un corto tiempo. Esto con el fin de captar la atención de los participantes sin profundizar en detalles técnicos o más específicos que podrían volverlo inapropiado para el público al que se desea llegar, volviéndolo tedioso o complicado.

Los contenidos del curso se imparten de manera magistral, mediante el uso de presentaciones para exponer y explicar los diferentes temas. El material se refuerza con el uso de videos que ilustran tópicos importantes y un documento anexo con enlaces a contenidos y recursos de interés para ampliar los conocimientos aprendidos. El curso tendrá una sección pública de preguntas en el entorno virtual de aprendizaje (EVA) que se elija, para que los participantes expongan dudas al profesor y las compartan entre ellos.

5.1.2 Diseño a nivel técnico

El curso está compuesto de videos en formato mp4 (un formato estándar y aceptado por la gran mayoría de medios digitales) y cada video abarca una sección. Esto le da una gran versatilidad para ser adaptado a diferentes entornos virtuales de aprendizaje (EVAs).

Desde el punto de vista de edición del curso, se buscó desarrollar por módulos los contenidos con el fin de facilitar su mantenimiento. Debido al vertiginoso avance tecnológico de las tecnologías de información y comunicación (TICs), las ciberamenazas aparecen, evolucionan y cambian constantemente, por lo que es recomendable una revisión de los contenidos al menos una vez cada seis meses para editarlos, agregar nuevos o eliminar los obsoletos. Para facilitar estas acciones se han grabado pequeños videos por cada filmina de cada presentación, videos que luego se unen mediante herramientas de edición para producir los contenidos de cada sección. De esta manera se ahorra tiempo y trabajo a la hora de realizar modificaciones y mejoras al curso, pues algunas secciones son extensas. Además, así se permite llevar un registro de versiones más detallado conforme el tiempo transcurra.

5.2 Estructura de contenidos de la solución

Lo primero que se realizó fue definir la estructura del curso; o sea, el índice de contenidos que será necesario para la elaboración de las presentaciones. Luego se identificaron las diferentes partes del mismo mediante una serie de revisiones para ir refinando y definiendo más la información requerida. La primera revisión la vemos a continuación:

Presentación

- Bienvenida al curso y presentación del profesor.
- Objetivo general y objetivos específicos.
- Presentación de los contenidos.

Contenidos del curso

Conclusiones y despedida

Con la definición del objetivo general y los objetivos específicos, se puede empezar a estructurar y esbozar los contenidos del curso. Por lo tanto, se definen los objetivos del curso quedando estos así:

Objetivo General

Proporcionar una formación introductoria a padres de familia y adultos al cuidado de menores de edad en el ámbito de la ciberseguridad enfocada en niños y adolescentes, que cree conciencia sobre las ciberamenazas a la que los menores de edad se ven expuestos al utilizar las TICs y cómo deben ser abordadas y manejadas.

Objetivos Específicos

- Definir qué es la ciberseguridad y su importancia en el mundo actual.
- Conocer la situación de la ciberseguridad en la actualidad tanto a nivel global como a nivel nacional.
- Identificar los distintos tipos de ciberamenazas a las que los menores de edad se ven expuestos, sus características y consecuencias.
- Identificar contenidos no aptos para menores de edad.

- Reconocer los lugares donde los menores de edad están más expuestos a ciberamenazas.
- Conocer el manejo apropiado de los diferentes tipos de ciberamenazas desde un enfoque preventivo.
- Conocer las acciones a realizar en caso de que una ciberamenaza se materialice en un incidente.
- Crear una cultura de la seguridad de la información en el hogar.

Con los objetivos específicos definidos, se identifican tres posibles secciones principales de contenidos: una sección introductoria donde se abarquen aspectos generales sobre la ciberseguridad, una segunda sección donde se describan y desarrollen los tipos de ciberamenazas y una tercera sección donde se aborde el manejo preventivo de las ciberamenazas y la respuesta a incidentes. Con esta información se genera una segunda revisión:

Presentación

- Bienvenida al curso y presentación del profesor.
- Objetivo general y objetivos específicos.
- Presentación de los contenidos.

Sección 1: Introducción

Sección 1.1: Ciberseguridad

Sección 1.2: Situación Actual de la ciberseguridad

Sección 2: Ciberamenazas

Sección 2.1: Tipos de ciberamenazas

Sección 2.2: Contenidos inapropiados y lugares de mayor riesgo.

Sección 3: Manejo de ciberamenazas

Sección 3.1: Prevención de ciberamenazas

Sección 3.2: Respuesta a incidentes

Conclusiones y despedida

Se realiza una tercera revisión donde se desarrollan los temas principales del curso, la cual queda así:

Presentación

- Bienvenida al curso y presentación del profesor.
- Objetivo general y objetivos específicos.
- Presentación de los contenidos.

Sección 1: Introducción

Sección 1.1: Ciberseguridad

- ¿Qué es la ciberseguridad?
- Clasificación de la ciberseguridad
- ¿Por qué es importante la ciberseguridad?
- Crear una cultura de la ciberseguridad
- Frases a eliminar de nuestro vocabulario

Sección 1.2: Situación actual de la ciberseguridad

- Datos a nivel mundial
- Amenazas a menores de edad
- Cibercrimen en Costa Rica
- Delitos más denunciados en Costa Rica en 2019
- Cibercrimen a menores de edad en Costa Rica
- ¿Qué dice la ley sobre el cibercrimen en menores de edad?
- Esfuerzos a nivel nacional
- Primera encuesta nacional de la niñez y la adolescencia

Sección 2: Ciberamenazas

Sección 2.1: Amenazas tecnológicas

- Amenazas físicas
- Amenazas por *software*

- Amenazas por redes públicas
- Contraseñas

Sección 2.2: Amenazas sociales

- Amenazas indirectas
- Amenazas directas
- *Ciberbullying*
- *Sexting*
- *Grooming*

Sección 2.3: Contenidos inapropiados y lugares de mayor riesgo

- Páginas de gore y violencia extrema, de drogas o pornografía
- Sitios web y aplicaciones más usadas por los menores de edad

Sección 3: Manejo de ciberamenazas

Sección 3.1: Cultura de la seguridad

- Crear una cultura de la ciberseguridad
- Tipos de mediación
- ¡Hay que involucrarse!

Sección 3.2: Prevención tecnológica

- Prevención física
- Descarga desde sitios seguros
- Antivirus
- Descarga de actualizaciones
- Contraseñas
- VPNs
- Programas de Control Parental

Sección 3.3: Prevención social

- ¡Sin miedo a la tecnología!
- La comunicación es vital

- Clasificación de productos tecnológicos
- Edades de acceso a redes sociales
- Empoderamientos de los menores de edad con respecto a su información
- Círculos de confianza

Sección 3.4: Respuesta a incidentes

- El daño ya está hecho
- Canales de denuncia

Conclusiones y despedida

Documento con anexos

Para la definición de estos temas y contenidos se ha echado mano principalmente de los conocimientos aprendidos a lo largo de la carrera y durante la revisión bibliográfica de los artículos primarios y la entrevista realizada; muchos de estos temas se complementaron con noticias y artículos adicionales. Así pues, podemos hacer una mención de las fuentes iniciales de la siguiente manera:

Sección 1.1: Artículos primarios citados en sección 1.7.4.1 (artículos 02 y 03), información recopilada durante la carrera (introducción a la seguridad de la información y otros).

Sección 1.2: Información recopilada durante la carrera (aspectos culturales, éticos, legales y regulatorios), consulta al Código penal costarricense, consultas a los sitios web de los organismos señalados y entrevista realizada.

Sección 2.1: Información recopilada durante la carrera (control de acceso, seguridad ambiental y física, seguridad en redes inalámbricas y dispositivos móviles).

Sección 2.2: Artículos primarios citados en sección 1.7.4.1 (artículos 01, 03, 04, 05 y 09).

Sección 2.3: Artículos primarios citados en sección 1.7.4.1 (artículo 01), primera encuesta nacional de la niñez y la adolescencia. Fundación Paniamor (2018) y entrevista realizada.

Sección 3.1: Artículos primarios citados en sección 1.7.4.1 (artículo 03), información recopilada durante la carrera (administración de sistema de gestión de seguridad de la información) y entrevista realizada.

Sección 3.2: Artículos primarios citados en sección 1.7.4.1 (artículos 02 y 10), información recopilada durante la carrera (seguridad en aplicaciones y seguridad y protocolos de comunicación).

Sección 3.3: Artículos primarios citados en sección 1.7.4.1 (artículos 01, 03 y 06).

Sección 3.4: Información recopilada de sitio de Fundación Paniamor para la denuncia (e-mentores).

Finalmente se realizó una cuarta revisión donde se completaron los contenidos a tratar. Se agregaron subsecciones introductorias, subsecciones para tratar conceptos importantes pero que no tenían cabida en las subsecciones ya tratadas. Finalmente, se agregaron temas complementarios y otros que no aparecían en la bibliografía original y que surgieron conforme el autor de este trabajo avanzó en la investigación.

Con esto, la estructura de contenidos quedó definida así:

Presentación

- Bienvenida al curso y presentación del profesor.
- Objetivo general y objetivos específicos.
- Presentación de los contenidos.

Sección 1: Introducción

Sección 1.1: La revolución digital

- El avance de las TICs
- La explosión de Internet
- El Internet de las cosas
- La automatización y la inteligencia artificial

Sección 1.2: Ciberseguridad

- ¿Qué es la ciberseguridad?
- Clasificación de la ciberseguridad
- ¿Por qué es importante la ciberseguridad?
- Crear una cultura de la ciberseguridad

- Adultos vs. menores de edad
- Frases a eliminar de nuestro vocabulario

Sección 1.3: Situación actual de la ciberseguridad

- Datos a nivel mundial
- Amenazas a menores de edad
- Cibercrimen en Costa Rica
- Delitos más denunciados en Costa Rica en 2019
- Cibercrimen a menores de edad en Costa Rica
- ¿Qué dice la ley sobre el cibercrimen en menores de edad?
- Esfuerzos a nivel nacional
- Primera encuesta nacional de la niñez y la adolescencia

Sección 2: Ciberamenazas

Sección 2.1: Algunos conceptos importantes

- Ingeniería social
- Lo que se sube a internet se queda en Internet
- La *deep web* y la *dark web*
- La huella digital, la identidad digital y la ciudadanía digital
- La tecnología es amoral

Sección 2.2: Amenazas tecnológicas

- Amenazas físicas
- Amenazas por *software*
- Amenazas por redes públicas
- Contraseñas

Sección 2.3: Amenazas sociales

- Amenazas indirectas
- Amenazas directas
- *Ciberbullying*
- *Sexting*

- *Grooming*
- *Sharenting*
- *Deep fakes* y *deep nude*

Sección 2.4: Contenidos inapropiados y lugares de mayor riesgo

- Páginas de gore y violencia extrema, de drogas o pornografía
- Sitios web y aplicaciones más usadas por los menores de edad
- ¿Y los videojuegos?

Sección 3: Manejo de ciberamenazas

Sección 3.1: Cultura de la seguridad

- Crear una cultura de la ciberseguridad
- Tipos de mediación
- ¡Hay que involucrarse!

Sección 3.2: Prevención tecnológica

- Prevención física
- Descarga desde sitios seguros
- Antivirus
- Descarga de actualizaciones
- Contraseñas
- VPNs
- Programas de Control Parental

Sección 3.3: Prevención social

- ¡Sin miedo a la tecnología!
- La comunicación es vital
- Clasificación de productos tecnológicos
- Edades de acceso a redes sociales
- Empoderamientos de los menores de edad con respecto a su información
- Círculos de confianza

Sección 3.4: Respuesta incidentes

- El daño ya está hecho
- Canales de denuncia

Conclusiones y despedida

Documento con anexos

Para esta parte cabe resaltar la información obtenida en el libro *Sálvese quien pueda* (Oppenheimer, 2018), para la recopilación de datos sobre el avance de la inteligencia artificial y el libro *Véndele a la mente, no a la gente* (Klaric, 2017), donde se explica desde el punto de vista de las neurociencias, el cerebro humano y sus debilidades a nivel de ingeniería social.

5.3 Elaboración técnica de los contenidos de la solución

Con la información recopilada en la sección anterior se procedió a la creación de las presentaciones. Para ello se utilizó el *software* Microsoft Power Point 2019, pues el autor de este trabajo conoce y maneja esta herramienta, la cual le otorga una gran libertad a la hora de crear contenido atractivo y con animaciones. También se adquirió la plantilla School Board para mejorar el apartado gráfico de las presentaciones, dándoles un acabado más profesional.

Para la edición de imágenes se empleó Adobe Illustrator CC 2018 versión portable, para realizar algunas vectorizaciones, y Microsoft Paint para realizar operaciones básicas como recortes o inclusión de texto.

Se realizaron anotaciones para algunas filminas que sirvieron de guía durante la grabación de las explicaciones cuando estas eran muy extensas.

Una vez completadas las presentaciones, se procedió a grabar la explicación de cada una, generando una grabación por cada filmina como se detalló anteriormente en la sección 5.1.2. El *software* de grabación empleado fue OBS Studio, una herramienta que permite un gran control sobre la producción, controles tales como filtros anti ruido, cantidad de *frames* por segundo (fps), canales de audio, codificación de video, resolución de pantalla, etc.

Realizadas las grabaciones, se procedió a concatenarlas para generar los videos de producción finales, eliminando cortes de transición y realizando ajustes de post producción. Para esto se empleó el *software* Wondershare Filmora X, una herramienta de edición de videos.

Finalmente, para la elaboración del documento anexo de enlaces a recursos complementarios se empleó Microsoft Power Point para ser consistentes en la imagen gráfica del trabajo, salvando el documento como un archivo en formato pdf.

5.4 Descripción de los contenidos de la solución

A continuación, se describen los contenidos tratados en cada sección del curso. Para este fin, se presenta la información en formato de tabla para cada sección principal. En la primera columna de la tabla figura el nombre de cada sección, subsección y tema; en la segunda columna se enumeran los tópicos expuestos.

Sección 1

Introducción al curso

Nombre	Descripción del contenido
1.1 La revolución digital	• Explicación el rápido avance tecnológico producto de la cuarta revolución industrial. • Exposición de cómo la tecnología está cambiando las normas de la sociedad generando grandes oportunidades, pero también grandes amenazas.
El avance de las TICs	• Se hace un breve repaso de la velocidad en que las TICs han avanzado en los últimos años • Se expone la precocidad con que los nativos digitales manejan las TICs, siendo el teléfono inteligente su principal dispositivo de procesamiento de información (Paniamor 2019).
La explosión de Internet	• Mediante el fechado de creación de algunas de las empresas de servicios de información más grandes del mundo se explica cómo internet ha revolucionado nuestros hábitos de consumo, de ocio, de trabajo y de socialización.

El Internet de las cosas	• Se explica el concepto de Internet de las cosas, ejemplificando mediante objetos de uso cotidiano.
La automatización y la inteligencia artificial	• Se explica qué es la inteligencia artificial y las múltiples aplicaciones en las que se está empleando. • Se manifiesta el peligro que representa la automatización en la destrucción de empleos y la necesidad de que las personas se reinventen y busquen los nuevos nichos laborales que la inteligencia artificial está creando y creará.
1.2 Ciberseguridad	• Se define el concepto de mundo físico real y del mundo virtual de Internet y cómo este último, al ser algo tan reciente, no permite muchas veces calibrar correctamente las amenazas y riesgos que este trae.
¿Qué es la ciberseguridad?	• Se explica el concepto de ciberseguridad dando una definición más apegada a la vida cotidiana de las personas. • Se enfatiza como fin último de la ciberseguridad el saber proteger la información personal y privada.
Clasificación de la ciberseguridad	• Se realiza una clasificación de la ciberseguridad desde el punto de vista del usuario final: Seguridad física, seguridad en las aplicaciones, seguridad en las redes y seguridad a nivel de las personas. • Se enfatiza como el error humano es clave en el 80% de los cibercrímenes, por lo tanto, este es el tema a trabajar más en el curso.

¿Por qué es importante la ciberseguridad?	• Se expone cómo con una mayor cantidad de dispositivos conectados a Internet, más consumo de servicios en línea y más posibilidades de conexión a redes, habrá una mayor probabilidad de ser víctima de ciberdelincuentes.
Crear una cultura de la ciberseguridad	• Se manifiesta por primera vez la urgente necesidad de empezar a generar una cultura de ciberseguridad en la crianza de los menores de edad para que estos puedan gozar de sus ventajas y beneficios del Internet de manera segura.
Adultos vs. menores de edad	• Se pone de manifiesto el gran desafío que los padres de familia modernos enfrentan debido a la gran velocidad en que las TICs evolucionan, provocando una brecha digital generacional cada vez mayor y generando problemas (muchas veces debido a desconocimiento) a la hora de aplicar un correcto cuidado parental en el mundo digital.
Frases a eliminar de nuestro vocabulario	• Se enfatiza en la importancia de eliminar de la mente las siguientes frases: *"Esto nunca me va a pasar a mí"* *"Mi seguridad es a prueba de todo"*
1.3 Situación actual de la ciberseguridad	• En esta sección se examina la situación de la ciberseguridad tanto en el mundo como en nuestro país. • Se desmitifica el concepto de ciberdelincuente como personas con altos conocimientos en informática,

	mostrando que las herramientas para hacer cibercrimen están al alcance de cualquiera.
Datos a nivel mundial	• Se exponen datos recopilados de agencias de ciberseguridad en el mundo. • Se expone cómo el cibercrimen se está volviendo la actividad ilegal de mayor crecimiento.
Cibercrimen en Costa Rica	• Se exponen cifras de ciberataques en Costa Rica recopiladas por agencias de ciberseguridad. • Se justifica la razón por la que muchas veces esta información no se escucha en los medios de comunicación.
Amenazas a menores de edad	• Se explica cómo una situación de pandemia generó un gran aumento en el consumo de pornografía infantil. • Se explica el fenómeno debido al confinamiento de menores de edad y su mayor tiempo conectados a las redes.
Cibercrimen a menores de edad en Costa Rica	• Se expone el preocupante aumento de las denuncias por cibercrímenes sexuales a menores de edad en cinco años. • Se desconoce el número real de los casos no denunciados.
Delitos más denunciados en Costa Rica 2019	• Se enlistan los delitos informáticos más denunciados en Costa Rica en 2019. Cinco de los ocho enunciados afectan directamente a menores de edad. • Se presentan las siguientes noticias de cibercrimen a menores de edad tomadas de medios de comunicación nacionales para ilustrar la situación:

	- Se dispara cifra de denuncias por seducir a menores en línea. (Alvarado, 2018). - Depravados se disfrazan de menores en redes para tener acercamientos sexuales con niños. (Solano, 2019). - Joven tica confiesa infierno cunado publicaron sus fotos estando desnuda. (Cabezas, 2017). - Mecánicos compartían pornografía infantil en grupo de WhatsApp de vecinos. (Solano, 2018). - Así cayó la red que distribuía fotos y vídeos de bebés abusados sexualmente. (Soto, 2019). - 20% de niños y adolescentes ticos fueron contactados por desconocidos en redes sociales. (Muñoz, 2020). - Amenazó a exnovia de 17 años con publicarle fotos íntimas tras violarla. (Agencia, 2020).
¿Qué dice la ley sobre el cibercrimen en menores de edad?	• Se cita el Artículo 167 bis del Código Penal de Costa Rica (SCIJ, 2020). • A pesar del reforzamiento de la ley, solo una denuncia se penalizó.
Esfuerzos a nivel nacional	• Se describe a fundación Paniamor como la principal abanderada en ciberseguridad para menores de edad. • Se mencionan otras instituciones tanto públicas como privadas y su contribución (MICITT, MEP, PANI, UCR, Movistar). • Se comenta que todavía no se posee un plan nacional que busque generar una cultura de la ciberseguridad desde las escuelas y colegios.

Primera encuesta nacional de la niñez y la adolescencia	• Se menciona la Primera Encuesta Nacional de la Niñez y Adolescencia y Tecnologías digitales en Costa Rica como un paso en la dirección correcta.

Tabla 1. Contenidos de la Sección1

Sección 2

Ciberamenazas

Nombre	Descripción del contenido
2.1. Algunos conceptos importantes	• Se exponen conceptos importantes que los asistentes en el curso necesitan para una mayor comprensión de cómo se maneja la información en el mundo virtual y el mundo físico, y cómo esto se relaciona con las ciberamenazas.
Ingeniería social	• Se explica qué es la ingeniería social. Se explora como está constituido nuestro cerebro desde una perspectiva de las neurociencias, identificando el cerebro límbico (cerebro emocional) como el principal punto de ataque de la ingeniería social. • Se explican las cuatro reglas de la ingeniería social y luego se les muestra a los PyT el vídeo: vídeo de ingeniería social (DOITSMART 2019). • Una vez visto el vídeo se les explica a los PyT cómo las cuatro reglas de ingeniería social vistas anteriormente se han aplicado en ese caso.
La *deep web* y la *dark web*	• Se les explica a los PyT qué es la *deep web* y la *dark web*, con el fin de mostrar cómo mucha información de carácter ilegal o

	que haya sido robada no puede ser rastreada o encontrada con facilidad.
Lo que se sube a Internet se queda en Internet	• Se refuerza la idea de que la información que subimos a Internet es casi imposible de borrar por completo, y que la correcta gestión de la información es responsabilidad del propietario de esa información.
La huella digital, la identidad digital y la ciudadanía digital	• Se definen los conceptos de huella digital, identidad digital y ciudadanía digital. Se define cómo estas crean y definen el "yo" digital a medida que se deja información en la red. • Se plantea la siguiente interrogante: ¿Qué información se puede dejar pública y que información no?
La tecnología es amoral	• Con la frase "la tecnología es amoral" se busca reforzar el concepto en los PyT de que, si bien el mundo digital alberga una gran cantidad de ventajas, nunca se debe de perder de vista que también alberga peligros y amenazas contra las que se debe estar siempre en guardia.
2.2. Amenazas Tecnológicas	• Retomando la clasificación de la ciberseguridad se procede a explicar las diferentes amenazas que pueden afectar a nivel tecnológico nuestra información.
Amenazas físicas	• Se explican las amenazas que pueden afectar nuestra información a nivel de nuestros dispositivos digitales.

Amenazas por *software*	• Se explican las amenazas que pueden afectar nuestra información mediante *malware*, y se dan algunos ejemplos.
Amenazas por redes públicas	• Se explica cuáles son los peligros y riesgos de conectar nuestros dispositivos móviles a una red pública de la cual desconocemos que nivel de seguridad tiene.
Contraseñas	• Se explica el riesgo que se corre cuando se utilizan contraseñas fáciles o repetitivas. • Se trata el problema que se genera cuando se necesita manejar una gran cantidad de contraseñas, todas diferentes y difíciles de recordar.
2.3. Amenazas sociales	• Se procede a explicar las diferentes amenazas que pueden, a nivel humano, vulnerar la información personal.
Amenazas indirectas	• Se define y dan ejemplos de las amenazas indirectas, describiendo el perfil de las personas que realizan estas prácticas.
Amenazas directas	• Se definen las amenazas directas.
Ciberbullying	• Se explica qué es el *ciberbullying*. • Se describen sus características. • Se citan las poblaciones más afectadas. • Se enumeran las motivaciones que tiene el acosador.

	• Se enumeran los síntomas que muestra el acosado. • Se explican cuáles son las consecuencias que el *ciberbullying* genera tanto en el acosador como en el acosado. • Se les muestra a los PyT el siguiente video de una campaña para concientizar sobre el *ciberbullying*: Vídeo de *Ciberbullying* (Orange España 2018).
Sexting	• Se explica qué es el *sexting.* • Se describen sus características. • Se explican qué razones hay detrás de la práctica del *sexting*. • Se explican los riesgos que lleva el practicar el *sexting*. • Se les muestra a los PyT un extracto del siguiente video de una campaña para concientizar sobre el *sexting* en menores de edad: Video sobre el *sexting* (AFM, 2018). • Se les muestra a los PyT un video donde se combina la práctica del *ciberbullying* con la práctica del *sexting*: Vídeo de *ciberbullying* y *sexting* combinados (Escalona, 2017).
Grooming	• Se explica qué es el g*rooming*. • Se describen sus características. • Se les muestra a los PyT el siguiente video de una campaña para concientizar sobre el *grooming* en menores de edad: Vídeo sobre el *grooming* (Entel, 2015). • Se explica el *modus operandi* de los delincuentes sexuales para realizar el *grooming*, exponiendo las diferentes fases del acoso realizadas mediante las reglas de ingeniería social que fueron explicadas anteriormente.
Sharenting	• Se explica en qué consiste el *sharenting* y qué consecuencias a largo plazo puede tener esta práctica en los niños a los que se les aplica cuando sean adultos.

	• Se les muestra a los PyT el siguiente video de una campaña para concientizar sobre el *sharenting*: Vídeo sobre *sharenting* (BA-CSIRT, 2019).
Deep fakes y *deep nude*	• Se exponen dos tecnologías muy recientes implementadas con inteligencia artificial que permiten la modificación de imágenes y vídeos indistinguibles de la versión original. • Se les muestra a los PyT un pequeño fragmento del siguiente video, el cual es una demostración de esta tecnología: Vídeo de *deepfake* (Shamook, 2020). • Se muestra esta noticia sobre el *deep nude* a los PyT y cómo se utilizó activamente en el poco tiempo que permaneció disponible: Roban fotos de redes y crean desnudos casi reales de mujeres y niños en un chat (Solano, 2020). • Finalmente, se insta a los PyT a imaginar posibles escenarios donde se combinen las diferentes ciberamenazas expuestas en esta sección y cómo los peligros asociados a estas se potencian aún más.
2.4. Contenidos inapropiados y lugares de mayor riesgo	• En esta sección se habla sobre los contenidos inapropiados para menores de edad y qué servicios y sitios frecuentan más en la red.
Páginas de gore y violencia extrema, de drogas o pornografía	• Se expone el riesgo de que los menores de edad accedan a contenidos no aptos para su edad.
	• Se muestran los porcentajes de uso de los diferentes servicios y sitios web utilizados por los menores de edad en Costa Rica,

Sitios web y aplicaciones más usadas por los menores de edad	identificando las redes sociales como de las más utilizadas y, por lo tanto, como el principal punto de entrada para los cibercriminales.
¿Y los videojuegos?	• Se presentan tres de los videojuegos más populares en la actualidad jugados por menores de edad (Minecraft, Fornite y Roblox). • Se explica en qué consisten, cuáles son sus características y beneficios y las potenciales ciberamenazas que tienen, esto con el fin de enseñar a los PyT la importancia de revisar los productos con que los menores juegan por más inocentes y beneficiosos que estos parezcan.

Tabla 2. Contenidos de la Sección 2

Sección 3

Manejo de ciberamenazas

Nombre	Descripción del contenido
3.1. Cultura de la seguridad	• Se vuelve a insistir con más detalle en la importancia de cultivar una cultura de la seguridad de la información. • Se enfatiza en la importancia de la prevención, pues cuando se produce un incidente es muy difícil remediarlo.
Crear una cultura de ciberseguridad	• Se explica en qué consiste una cultura de seguridad de la información y cómo busca maximizar los beneficios que las TICs minimizando las amenazas. • Se busca concientizar a los padres de familia sobre la importancia de cultivar buenos hábitos en el manejo de la información por parte de todos los miembros del hogar, no solo los menores de edad, pues el cibercrimen es un problema de nos afecta a todos.

Tipos de mediación	• Se explican los cuatro tipos de mediación parental y se señala cuál es el más adecuado y mejor para educar a los menores de edad en el mundo digital.
¡Hay que involucrarse!	• Se indica como punto clave para ser un mediador parental efectivo el involucrarse con los menores de edad en el manejo de las TICs, predicando con el ejemplo. • Se enfatiza en la importancia de aprender sobre las preferencias y gustos de los menores de edad con las TICs. • Recolectar toda la información posible sobre los menores de edad bajo un clima de confianza ayudará a los PyT a identificar amenazas tempranamente.
3.2. Prevención tecnológica	• Esta sección se enfoca en la parte más importante de la ciberseguridad: ¿cómo protegemos nuestra información?
Prevención física	• Se describen diferentes sistemas de respaldo de la información en caso de falla de un dispositivo. • Se describen programas y servicios remotos de cifrado antirrobo en caso de que se necesite guardar información sensible en nuestros dispositivos móviles.
Descarga desde sitios seguros	• Se explica la importancia de descargar aplicaciones móviles desde sitios seguros (tiendas oficiales de aplicaciones, sitios de fabricantes).

Antivirus	• Se explica la importancia de tener siempre un programa antivirus activo y actualizado en todos dispositivos que se tengan. Se dan algunos ejemplos de programas antivirus recomendables.
Descarga de actualizaciones	• Se explica la importancia de tener siempre los sistemas operativos al día, pues muchas actualizaciones traen parches de seguridad para vulnerabilidades detectadas.
Contraseñas	• Se enumeran las diferentes reglas para la creación de contraseñas seguras. Se realiza una demostración del sitio web de una empresa de ciberseguridad que permite probar la robustez de contraseñas: Kaspersky Password Checker. • Finalmente, se explica en qué consiste un programa administrador de contraseñas y cómo ayuda a resolver el problema de manejar una gran cantidad de contraseñas complejas y únicas.
VPNs	• Se explica en que consiste una VPN y cómo brinda seguridad de navegación sin importar la seguridad de la red pública a la que se esté conectado. • Se muestra a los PyT un video ilustrativo para complementar lo estudiado sobre una VPN: Vídeo sobre las VPN (Surfshark, 2020).
Programas de Control Parental	• Se explica qué son los programas de mediación parental y sus funcionalidades, destacando los beneficios que estos nos pueden ofrecer siempre que los manejemos desde un enfoque de mediación activo.

	• Se complementa la información con un video: Vídeo de programa de control parental.
3.3. Prevención social	• En esta sección se exponen los métodos para desarrollar un control parental efectivo ante ciberamenazas de tipo social.
¡Sin miedo a la tecnología!	• Se vuelve a insistir en la importancia de que los padres de familia se instruyan y aprendan sobre las TICs.
La comunicación es vital	• Se hace hincapié en la importancia de que los padres de familia y tutores tengan un canal de confianza abierto hacia los menores de edad, para poder establecer con ellos negociaciones proactivas. • Se busca llegar a un equilibrio entre la libertad y privacidad de parte del menor de edad y seguridad y tranquilidad de parte del padre de familia. • Una relación de confianza con el menor de edad es el arma de ciberseguridad más efectiva que existe.
Clasificación de productos tecnológicos	• Se identifican distintas señales para identificar si un producto tecnológico es apropiado para un menor de edad o no lo es.
Edades de acceso a redes sociales	• Se recomienda una edad mínima de trece años para el acceso a redes sociales.

Empoderamientos de los menores de edad	• Se muestra la importancia de empoderar a los menores de edad en la protección y cuidado de su huella e identidad digital, pues de adultos ellos serán los únicos responsables de las mismas. Se dan varios ejemplos de tópicos que los PyT pueden enseñar a los menores.
Círculos de confianza	• Se enseña, mediante un ejemplo, cómo se puede clasificar la información personal, no personal y el acceso a esta por terceros según el nivel de confianza que una persona tenga con el propietario de la información.
3.4. Respuesta a un incidente	• En esta sección se contempla qué hacer si se materializó una amenaza a nivel social.
El daño ya está hecho	• A nivel de *ciberbullying* se habla del protocolo contra el ciberbullying implementado por el MEP. Se dan una serie de acciones que los PyT pueden realizar con el acosador, el acosado y los espectadores. • A nivel de g*rooming* y *sexting*, se dan una serie de pasos para realizar la denuncia y qué acciones evitar.
Canales de denuncia	• Se muestran los canales del PANI y el OIJ para solicitar ayuda o realizar denuncias.

Tabla 3. Contenidos de la Sección 3

Documento de anexos

Se trata de un documento en formato PDF accesible para los PyT, en el que se dejan diferentes tipos de recursos y sitios web clasificados por categorías, con información útil en el proceso de aprendizaje de la ciberseguridad orientada a menores de edad.

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

Tomando como guía el objetivo general de este trabajo y los cuatro objetivos específicos, se presenta las siguientes conclusiones

1. Se identifican las ciberamenazas a las que los menores de edad se ven expuestos. Se agrega el *sharenting* como una nueva ciberamenaza a las ya identificadas en los artículos primarios, pues los autores de estos no la mencionan. Esto puede deberse a que inicialmente el *sharenting* se consideraba una actividad familiar inocua y no un problema de seguridad a largo plazo, demostrando lo poco que se sabe de cómo la información que se ve inofensiva hoy puede ser peligrosa mañana ante la aparición de nuevas tecnologías.

2. Se comprenden las ciberamenazas identificadas, sus características e impacto, así como el manejo y prevención de estas. Con en análisis realizado, se reconocen las ciberamenazas de tipo social -donde el blanco de ataque principal son las personas y no la infraestructura tecnológica- como las más peligrosas para los menores de edad, debido a que son más agresivas a nivel personal. El daño que generan va más allá de lo material, puede producir trastornos psicológicos o suicido al ser aplicado en personas que están en formación, e incidir en la definición de su personalidad e identidad.

3. Se seleccionan los temas, metodologías, materiales y contenidos que se implementarán para el curso. Se tuvo que realizar un ajuste en la metodología debido a que la pandemia de COVID-19 frustró todo intento de impartir el curso de manera presencial.
   Al final, esto resultó en algo positivo, pues al elaborarse como un curso de modalidad virtual asíncrona, este se volvió más versátil y con más posibilidades de llegar a más personas con una adecuada divulgación.

4. Se investigan los temas a desarrollar en el curso. La investigación fue un proceso complicado, no por la dificultad del tema o falta de fuentes, sino porque conforme la investigación avanza se generan interrogantes sobre la conveniencia de agregar más contenidos al curso o profundizar más en algunos temas, de tal manera que, si no se tiene claro la delimitación de los contenidos, se corre el peligro de volverlo demasiado extenso o especializado, incumpliendo así con el objetivo principal del trabajo. Sin embargo, esto también significa que para futuros desarrollos en el campo de la alfabetización digital y concientización aún hay mucho trabajo por hacer.

5. Se elabora un curso introductorio en ciberseguridad orientado a padres de familia y tutores de menores de edad en general al haber alcanzado cumplir de manera satisfactoria los objetivos específicos planteados en el trabajo. Se ha conseguido un curso cuyo mantenimiento y actualización de temas puede realizarse de manera sencilla, algo nada complicado de hacer si se gestiona mediante algún sistema de control de versiones (SVG). Los materiales pueden ser fácilmente adaptados a cualquier EVA.

6.2 Recomendaciones

6.2.1. Recomendaciones desde el punto de vista técnico

- En el apartado de grabación de las sesiones del curso se recomienda el uso de una cabina de estudio de grabación, pues es inevitable que se cole en la grabación algo de sonido ambiental, aunque se grabe en la madrugada para evitar al máximo sonidos del exterior. La persona encargada de la grabación debe tener o desarrollar habilidades de locución para dar un discurso fluido y carente de muletillas.
- En el apartado gráfico, se recomienda ya sea una mejor formación en herramientas de animación o tener personal en esta área para poder realizar producciones de mayor atractivo y calidad.
- Se recomienda el uso de un computador potente que dé prestaciones tanto para el rápido renderizado de animaciones y codificación de video, tareas que pueden durar horas si no se cuenta con un buen equipo. También un ancho de banda en Internet potente para poder mover archivos de video grandes.

6.2.2. Recomendaciones desde el punto de vista metodológico

Este curso debe verse como un primer paso base en la elaboración de un conjunto de producciones de diferentes tipos que funcionen de manera holística para poder llegar al mayor público posible y comunicar el mensaje de manera efectiva. De nada sirve tener materiales educativos e informativos si nadie los conoce.

Algunos ejemplos de metodologías que pueden hacer sinergias son: canales de YouTube dirigidos a informar sobre noticias y eventos recientes que ocurran en el mundo de la ciberseguridad, buscando siempre eliminar la desinformación en la ciudadanía. También la elaboración de talleres y videos cortos donde se examinen a detalle productos de ciberseguridad como VPNs o comparación de productos como *software* de cuidado parental.

6.2.3. Recomendaciones desde el punto de vista académico

Se debe buscar un mayor trabajo interdisciplinario y no exclusivo de una sola área. Actualmente se encuentran trabajos o muy técnicos, desde las ciencias computacionales, o muy a nivel social desde las ciencias de la educación. Una unión de ambas visiones generaría trabajos más ricos en contenido y calidad.

Finalmente, cabe recalcar que, si determinamos que el error humano es el mayor causante de problemas en la seguridad de la información, entonces la importancia de continuar avanzando en el desarrollo de una cultura de la ciberseguridad para la ciudadanía es más que evidente.

De nada sirve tener una infraestructura de seguridad tecnológica de punta y cercana a la perfección si las personas que la van a utilizar siguen escribiendo su contraseña personal debajo del teclado.

Capítulo 7. Trabajos a futuro

El presente trabajo busca dar un primer paso hacia la creación de una cultura de la seguridad de la información y el uso seguro y responsable de los productos y servicios que ofrecen las TICs, educando a la ciudadanía desde edades tempranas. El autor de este trabajo presenta una serie de posibles trabajos futuros en orden de complejidad, cuyo fin último sería alcanzar estos objetivos a nivel nacional incluyendo a diversos actores de la sociedad:

1- Elaboración de un curso introductorio en ciberseguridad orientado a PyT (trabajo actual).
2- Aplicación del curso en una institución educativa con la recolección de resultados para el mejoramiento del mismo. Si la institución muestra interés, puede implantarse como parte de la formación dada por la institución como un valor agregado, mejorándolo y actualizándolo con la retroalimentación recibida.
3- Elaboración de materiales educativos para la enseñanza de la ciberseguridad a menores de edad por parte de educadores en una institución educativa. Al estar dirigido a menores de edad, este trabajo ofrece una magnífica oportunidad para la colaboración interdisciplinaria, pues se necesitaría además del profesional en informática, al menos a un pedagogo y un sicólogo. Además, podrían tratarse otros problemas relacionados con las TICs, tales como las adicciones a Internet, a los videojuegos, a los trastornos del sueño por el uso de pantallas, etc. Luego podría repetirse el trabajo del punto 2 para otra investigación o hacerlo todo en uno si se cuenta con el tiempo y los recursos.
4- Elaboración de diferentes propuestas para la mejora de la ciberseguridad a nivel de una institución educativa. De aquí pueden salir diferentes tipos de trabajos tales como la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) generando políticas para la correcta gestión de la información sensible que la institución educativa maneje, tanto a nivel administrativo como estudiantil. Otro trabajo sería un plan (y luego su implementación) para la mejora de la seguridad desde el punto de vista de la arquitectura e infraestructura tecnológica de la institución.
5- Si se han logrado realizar los proyectos anteriormente expuestos en una institución, esta podría servir como modelo a replicar en otras instituciones y, eventualmente, luego de varios años de mejora, el poder presentar un plan ante el Ministerio de Educación Pública para ser considerado como parte de una iniciativa a nivel nacional.

Referencias

1. A Favor de lo Mejor. (2018). *Sexting.* Recuperado de: enlace a la fuente
2. Agencia. (2020). “Amenazó a exnovia de 17 años de publicarle fotos íntimas tras violarla”. *Crhoy.com*. Recuperado de: enlace a la fuente
3. Alvarado, J. (2018). “Se dispara cifra de denuncias por seducir a menores en línea”. *Crhoy.com*. Recuperado de: enlace a la fuente
4. BA-CSIRT. (2019). ¿Qué es el *sharenting*? Recuperado de: enlace a la fuente
5. Cabezas, Y. (2017). “Joven tica confiesa infierno cuando publicaron sus fotos desnuda”. *Crhoy.com*. Recuperado de: enlace a la fuente
6. DOITSMART. (2019). *Así se hace la ingeniería social*. Recuperado de: enlace a la fuente
7. Entel. (2015). *Campaña prevención Grooming -PDI*. Recuperado de: enlace a la fuente
8. Escalona, F. (2017). *Campaña: Tus mensajes también lastiman*. Recuperado de: enlace a la fuente
9. ESET Latinoamérica. (2015). *¡Protege a tus hijos en internet con ESET Parental Control para Android!* Recuperado de: enlace a la fuente
10. Fundación Paniamor. (2019). *Usos de tecnología móvil y violencia en línea*. Recuperado de: enlace a la fuente
11. Klaric, J. (2017) *Véndele a la mente, no a la gente: Neuroventas: una ciencia nueva para vender más hablando menos.* (2 ed.). México: Ediciones Culturales Paidós.
12. Muñoz, F. (2020). *20% de niños y adolescentes ticos fueron contactados por desconocidos en redes sociales. Monumental*. Recuperado de: enlace a la fuente
13. Oppenheimer, A. (2018). *¡Sálvese quien pueda!: El futuro del trabajo en la era de la automatización.* (primera edición). México: Penguin Random House Grupo Editorial.
14. Orange España. (2018). *Niños ciberacosadores. Lo que no sabes de tus hijos*. Recuperado de: enlace a la fuente
15. SCIJ. (2021). *Reforma de los artículos 196,196 BIS, 230, 293 y 295 y adición al artículo 167 BIS al código penal*. Recuperado de: enlace a la fuente
16. Shamook (2020) *Burt Reynolds is James Bond in Dr. No [DeepFake].* Recuperado de: enlace a la fuente.
17. Solano, J. (2019). “Depravados se disfrazan de menores en redes para tener acercamientos sexuales con niños”. *Crhoy.com*. Recuperado de: enlace a la fuente
18. Solano, J. (2018). “Mecánicos compartían pornografía infantil en grupo de WhatsApp de vecinos”. *Crhoy.com*. Recuperado de: enlace a la fuente

19. Solano, J. (2020). *Roban fotos de redes y crean desnudos casi reales de mujeres y niños en un chat*. Recuperado de: enlace a la fuente
20. Soto, J. (2019). “Así cayó la red que distribuía fotos y vídeos de bebés abusados sexualmente*”. Crhoy.com.* Recuperado de: *enlace a la fuente*
21. Surfshark. (2020). *¿Qué es una VPN?* Recuperado de: enlace a la fuente.