

UNIVERSIDAD CENTRAL DE NICARAGUA

“Agnitio Ad Verum Ducit”

Facultad de Ingeniería en Sistemas

Sede Central



Monografía para optar al título de ingeniero en sistemas

Título: Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025.

Autor (es):

- Alexander Antonio Guillen Ruiz N° Carnet: 201930010274
- Eddy Miguel Guzmán N° Carnet: 09-01954-07-j

Asesor (a): Ing. Beatriz del Carmen Franco Escorcia

Institución (es): UCN

Fecha de Presentación: 2 de marzo

MANAGUA – NICARAGUA

Agradecimiento

Queremos expresar nuestro más sincero agradecimiento a todas aquellas personas e instituciones que, de una manera u otra, han contribuido a la realización de este proyecto.

En primer lugar, agradecemos a Dios por darnos la salud, la fortaleza y la perseverancia necesarias para llevar a cabo esta investigación. Sin su guía y bendición, este logro no habría sido posible.

A nuestras familias, por su apoyo incondicional, paciencia y motivación en cada etapa de este proceso. Gracias por creer en nosotros y brindarnos el ánimo necesario para seguir adelante.

A nuestra tutora, Beatriz del Carmen Franco Escorcía, por su valiosa orientación, paciencia y compromiso con nuestro desarrollo académico. Su experiencia y dedicación fueron esenciales para mejorar cada aspecto de este trabajo.

A nuestros amigos y compañeros de estudio, quienes nos acompañaron en esta travesía universitaria. Sus consejos, debates y apoyo moral hicieron que este proceso fuera una experiencia enriquecedora.

A nuestra universidad, por brindarnos la oportunidad de formarnos profesionalmente y proporcionarnos las herramientas necesarias para el desarrollo de este proyecto. A los docentes y personal administrativo, por su dedicación y esfuerzo durante nuestra formación académica.

A la comunidad de Monte Fresco, por permitirnos desarrollar esta investigación y ser la inspiración detrás de nuestro trabajo. Sus aportes fueron clave para comprender las necesidades de formación en ciberseguridad y mejorar nuestra propuesta educativa.

Finalmente, a todas las personas que contribuyeron con sus conocimientos, experiencias y apoyo moral, les extendemos nuestro más profundo agradecimiento.

Dedicatoria

Dedico este trabajo, en primer lugar, a Dios, por ser mi guía y fortaleza en cada paso de este camino. Sin su sabiduría y bendiciones, este logro no habría sido posible.

A mi madre, Mirtha Elizabeth Ruiz Zamora, por su amor incondicional, sacrificio y apoyo inquebrantable. Gracias por enseñarme el valor del esfuerzo, la perseverancia y por ser mi inspiración en cada desafío.

A mis hermanos, Mirtha Guillen y Jocsan Guillen, por su compañía, consejos y motivación constante. Su apoyo ha sido fundamental para seguir adelante y alcanzar mis metas.

A toda mi familia, por su amor, paciencia y aliento en los momentos más difíciles. Gracias por estar siempre presentes y por creer en mí.

A mis amigos, por su compañía, apoyo incondicional y por brindarme momentos de alegría en este proceso. Su amistad ha sido un pilar fundamental en mi camino académico y personal.

A mis docentes y compañeros, por su orientación, consejos y colaboración a lo largo de esta etapa académica. Su apoyo ha sido clave para mi crecimiento profesional y personal.

A la comunidad de Monte Fresco, cuya necesidad de formación en ciberseguridad inspiró este proyecto. Espero que este trabajo contribuya a fortalecer su conocimiento y mejorar su seguridad digital.

Finalmente, a todas las personas que, de una u otra manera, me apoyaron en este proceso, brindándome palabras de aliento, confianza y motivación. A todos ustedes, mi más sincera gratitud.

Alexander Antonio Guillen Ruiz

Dedicatoria

Este proyecto está dedicado con todo mi amor y gratitud a mi familia. A mi esposa, por su apoyo, paciencia y comprensión durante todo este proceso. A mi madre, por su sabiduría, enseñanzas y por inculcarme los valores que me han guiado a lo largo de mi vida. Tu fortaleza y dedicación han sido una fuente constante de inspiración para mí, y sin tu ejemplo, no habría llegado hasta aquí.

A mis hijas, quienes son mi mayor motivación y alegría. Ustedes me enseñan cada día la importancia de la perseverancia y el amor incondicional. Espero que este logro les demuestre que con esfuerzo y dedicación, todo es posible. Su curiosidad y entusiasmo por aprender me impulsan a ser mejor cada día y a seguir adelante, incluso cuando las cosas se ponen difíciles.

A mis amigos y colegas, quienes han estado a mi lado en este viaje académico. Su apoyo, consejos y palabras de aliento han sido invaluable. Gracias por compartir conmigo sus conocimientos y experiencias, y por hacer de este camino uno más llevadero y enriquecedor.

Y sobre todo, dedico este trabajo a Dios, quien siempre guía mis pasos y me brinda la fortaleza para seguir adelante. Agradezco su presencia en mi vida, su protección y las bendiciones que me ha otorgado. Sin su guía y apoyo, este proyecto no habría sido posible. Su amor y misericordia me han dado la fuerza para superar los obstáculos y alcanzar mis metas.

Finalmente, quiero agradecer a todas las personas que, de una u otra manera, han contribuido a la realización de este proyecto. A mis profesores y mentores, por su dedicación y compromiso en mi formación académica. A la comunidad de Monte Fresco, por su colaboración y disposición para participar en este estudio. Este logro es también de ustedes, y espero que los resultados de este trabajo contribuyan a mejorar la seguridad digital y el bienestar de nuestra comunidad.

Eddy Miguel Guzmán



UNIVERSIDAD CENTRAL DE NICARAGUA

"Agnitio Ad Verum Ducit"

CARTA AVAL TUTOR METODOLOGO/CIENTIFICO (A)

Lic. Karen López H.
Decana de la Facultad de Ingeniería en Sistemas
UCN – Sede Central
Su Despacho

Por medio de la presente hago constar que he verificado el informe final del trabajo monográficos elaborado por el/los egresados(s)

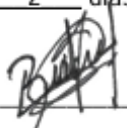
Br. Alexander Antonio Guillen Ruiz con número de carné 201930010274

Br. Eddy Miguel Guzmán con número de carné 09-01954-07-j

Para optar al título de Ingeniería en sistemas, cuyo título de la Monografía es:
Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, Managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025.

El cual considero que cumple con los requisitos metodológicos exigidos por el **CAPÍTULO VIII FORMAS DE CULMINACION DE ESTUDIO** del reglamento académico; para ser evaluada por el Comité Evaluador.

En La Ciudad de managua a los 2 días del mes de marzo del año 2025.

Ing. 

Tutor(a) Metodológico/Científico: Ing. Beatriz Franco Escorcia

CC: Archivo.

1. Resumen

Este estudio desarrolló un prototipo de plataforma educativa en ciberseguridad para la comunidad de Monte Fresco, en el municipio de Villa El Carmen, Managua, Nicaragua. La investigación abordó la vulnerabilidad de la población ante amenazas cibernéticas como fraudes, robo de identidad y malware, debido a la limitada alfabetización digital en la región, lo que aumenta el riesgo de exposición a ataques informáticos.

El proyecto tuvo como objetivo integrar el prototipo de una plataforma de aprendizaje basada en Canvas LMS para facilitar la enseñanza de ciberseguridad en la comunidad, dirigida a jóvenes y adultos. Para ello, se identificaron las necesidades de formación mediante entrevistas y observaciones. Con base en estos hallazgos, se diseñó una interfaz intuitiva y accesible, adaptada a administradores, profesores y estudiantes, garantizando una experiencia de usuario eficiente.

Se desarrollaron módulos educativos que abordan temas como phishing, malware y buenas prácticas de seguridad en línea, proporcionando contenido teórico y práctico para mejorar la protección digital de los participantes.

El prototipo busca fortalecer los conocimientos en ciberseguridad y reducir los riesgos digitales en la comunidad. Su implementación potencial podría servir como un modelo replicable en otras comunidades con desafíos similares en materia de seguridad informática.

2. Tabla de Contenido

1.	Resumen	6
2.	Tabla de Contenido	7
3.	Índice de Tablas	8
4.	Índice de figuras.....	9
5.	Introducción.....	10
5.1.	Identificación del Problema de Investigación (Antecedentes y Contexto del Problema)	11
	Programa de Ciberseguridad del Banco Interamericano de Desarrollo (BID)	12
5.2.	Objetivos.....	14
5.2.1.	General	14
5.2.2.	Objetivos Específicos.....	14
5.3.	Preguntas de Investigación.....	14
5.4.	Justificación	15
5.5.	Limitaciones.....	17
5.6.	Supuestos Básicos.....	19
5.7.	Categorías, temas y patrones emergentes de la investigación	19
5.7.1.	Categorías.....	19
5.7.2.	Temas Clave	20
5.7.3.	Patrones Emergentes	21
6.	Perspectiva Teórica	22
6.1.	Estado del Arte	22
6.2.	Perspectiva Teórica Asumida.....	25
6.2.1.	Teoría del Aprendizaje Constructivista	25
6.2.2.	Teoría del Capital Social	25
6.2.3.	Teoría de la Alfabetización Digital.....	26
6.2.4.	Enfoque Participativo	26
6.2.5.	Teoría de la Gamificación	27
6.2.6.	Integración de las Perspectivas Teóricas	27
7.	Metodología.....	28
7.1.	Enfoque cualitativo asumido y su justificación	28
7.2.	Muestra Teórica y Sujetos del Estudio	28
7.3.	Muestra	28

7.3.1. Sujeto de estudio	29
7.4. Métodos y Técnicas de Recolección de Datos.....	29
7.4.1. Método.....	29
7.4.2. Técnica	30
7.5. Criterios de Calidad Aplicados: Credibilidad, Confiabilidad y Triangulación	31
7.5.1. Credibilidad	31
7.5.2. Confiabilidad	31
7.5.3. Triangulación.....	32
7.6. Métodos y Técnicas para el Procesamiento de Datos y Análisis de Información	32
8. Discusión de hallazgos y resultados.....	34
8.1. Necesidades de Formación en Ciberseguridad	34
8.2. Integración del Prototipo de la Plataforma	34
8.3. Incorporación de contenido interactivo y adaptado.....	35
8.4. Resultados finales.....	35
8.5. Recomendaciones.....	36
9. Referencias.....	37
10. Anexos o Apéndices	38
Diseño del sistema informático	38

3. Índice de Tablas

Tabla 1: Matriz de Reducción de Datos	52
Figura 2: Cronograma de Actividad.....	54
Tabla 3: Presupuesto.....	55

4. Índice de figuras

Figura 1: Diagrama de Entidad-Relación.....	41
Figura 2: Diagrama de Casos de Uso.....	43
Figura 3: Diagrama de Secuencia	44
Figura 4: Interfaz de Administrador	49
Figura 5: Interfaz de Profesor	50
Figura 6: Interfaz de Estudiante	51
Figura 7: Entrevistas semiestructuradas.....	57
Figura 8: Entrevista Semiestructurada.....	58
Figura 9: Entrevista Semiestructurada.....	59
Figura 10: Resultados de la Entrevista	60
Figura 11: Resultados de la Entrevista	61
Figura 12: Resultados de la Entrevista	62
Figura 13: Resultados de la Entrevista	63
Figura 14: Resultados de la Entrevista	64
Figura 15: Resultados de la Entrevista	65
Figura 16: Resultados de la Entrevista	66
Figura 17: Resultados de la Entrevista	67
Figura 18: Resultados de la Entrevista	68
Figura 19: Resultados de la Entrevista	69
Figura 20: Resultados de la Entrevista	70

5. Introducción

La creciente dependencia de las tecnologías digitales en la vida cotidiana y el trabajo ha expuesto a comunidades de todo el mundo a una serie de riesgos cibernéticos, como fraudes, robo de identidad y acceso no autorizado a información privada. En Nicaragua, la formación en ciberseguridad es aún limitada, particularmente en áreas rurales o semiurbanas como Monte Fresco, Villa El Carmen. Esta falta de conocimiento aumenta la vulnerabilidad frente a amenazas como el phishing, malware y violaciones de datos, que afectan tanto a individuos como a pequeñas organizaciones locales.

En el casco urbano de Managua, se encuentra la comunidad de Monte fresco ubicada en Villa El Carmen, Managua. La comunidad de Monte Fresco, ubicada en Villa El Carmen, Managua, enfrenta desafíos específicos debido a su limitada infraestructura tecnológica y conectividad a internet. La diversidad demográfica, con variaciones significativas en los niveles de educación y acceso a tecnologías, agrava esta situación. Además, la ausencia de formación en ciberseguridad expone a sus habitantes a riesgos digitales y limita su participación en la economía digital.

El desarrollo de un prototipo educativo en ciberseguridad abordó directamente esta brecha, proporcionando una herramienta accesible y personalizada para capacitar a los habitantes. Este proyecto no solo fomenta la alfabetización digital en temas de seguridad, sino que también refuerza la capacidad de la comunidad para protegerse frente a riesgos informáticos, contribuyendo a su empoderamiento y seguridad digital.

La relevancia de este proyecto radica en su potencial para cerrar la brecha digital en términos de seguridad y educación, aspectos esenciales para un desarrollo sostenible en la era digital. La colaboración con instituciones educativas locales y el Ministerio de Educación (MINED)

es crucial para proporcionar el respaldo institucional necesario y asegurar que el proyecto se alinee con las políticas educativas nacionales. Además, la participación activa de la comunidad y la formación de facilitadores locales son factores clave para el éxito y la sostenibilidad del proyecto a largo plazo.

5.1. Identificación del Problema de Investigación (Antecedentes y Contexto del Problema)

En Nicaragua, varias iniciativas recientes se han desarrollado para fortalecer la capacitación en ciberseguridad, que pueden servir como antecedentes relevantes para tu investigación. A continuación, se resumen algunas de ellas:

Laboratorios de Ciberseguridad en INATEC

El Instituto Nacional Tecnológico (INATEC) ha inaugurado laboratorios especializados en ciberseguridad, como el del Centro Tecnológico Manuel Olivares Rodríguez. Estos espacios están destinados a la formación de técnicos en áreas clave de ciberseguridad, con el objetivo de prevenir y responder a amenazas cibernéticas. Además, INATEC impulsa la capacitación de docentes para ampliar el alcance de estos conocimientos en centros tecnológicos a nivel nacional, con el respaldo de la cooperación suiza (COSUDE) (INATEC, 2023). Estas iniciativas forman parte de una estrategia integral para acompañar la transformación digital del país y mitigar los crecientes riesgos cibernéticos (Nica, 2023)

Colaboración entre Fortinet y la Universidad Americana (UAM)

La empresa global de ciberseguridad Fortinet se ha asociado con la Universidad Americana (UAM) para ofrecer cursos y certificaciones en ciberseguridad a través del programa Fortinet Network Security Academy (Fortinet, 2023) . Este programa tiene como objetivo atender la creciente demanda de profesionales capacitados mediante certificaciones reconocidas internacionalmente, permitiendo a los estudiantes desarrollar habilidades técnicas avanzadas y mejorar su competitividad en el mercado laboral (UAM, 2023).

Educación y sensibilización en ciberseguridad

Los cursos impartidos por INATEC y otras instituciones también incluyen la alfabetización digital como un componente clave para reducir vulnerabilidades como el phishing y otras amenazas comunes. Estas capacitaciones buscan empoderar tanto a estudiantes como a comunidades locales, proporcionándoles herramientas para afrontar los riesgos asociados al uso creciente de tecnologías digitales en distintos sectores (Nica, 2023).

Programa de Ciberseguridad del Banco Interamericano de Desarrollo (BID)

El Banco Interamericano de Desarrollo (BID) ha implementado un programa de fortalecimiento de la ciberseguridad en América Latina y el Caribe, el cual incluye capacitaciones para instituciones gubernamentales y empresas privadas. Este programa busca mejorar la preparación ante ataques cibernéticos y fomentar una cultura de seguridad digital en la región. En Nicaragua, el BID ha colaborado con diversas instituciones para desarrollar estrategias de protección digital y reforzar la infraestructura de ciberseguridad (BID, 2023).

Iniciativas de la OEA en ciberseguridad

La Organización de los Estados Americanos (OEA) ha impulsado diversas iniciativas de capacitación en ciberseguridad en la región, incluyendo programas de formación en línea y talleres presenciales. A través del Programa de Seguridad Cibernética, la OEA ha trabajado con gobiernos y universidades para desarrollar capacidades en la identificación y mitigación de amenazas digitales. En Nicaragua, estas iniciativas han fortalecido la cooperación entre el sector público y privado en la protección de datos y sistemas informáticos (ONU, 2021).

5.2. Objetivos

5.2.1. General

Desarrollar un prototipo de una plataforma de aprendizaje de ciberseguridad que permita la enseñanza en la comunidad de Monte Fresco, Villa El Carmen, Managua.

5.2.2. Objetivos Específicos

- Identificar las necesidades de formación en ciberseguridad de la comunidad de Monte Fresco, Villa El Carmen.
- Integrar el prototipo de una interfaz para el aprendizaje de ciberseguridad en la plataforma basado en Canvas LMS considerando los roles administradores, profesor y estudiante.
- Desarrollo del prototipo de la plataforma basado en Canvas LMS de forma intuitiva.
- Realizar los módulos educativos enfocados phishing y malware.

5.3. Preguntas de Investigación

¿Cuáles son las necesidades de formación en ciberseguridad de los habitantes de la comunidad de Monte Fresco, Villa El Carmen?

¿Cómo debe integrarse un prototipo interactivo para garantizar que sea funcional, accesible y didáctico?

¿Cuál es el impacto del prototipo en los conocimientos y prácticas de ciberseguridad de los participantes del grupo piloto?

5.4. Justificación

En la actualidad, el acceso y uso de tecnologías digitales se han vuelto fundamentales para la comunicación, la educación y el trabajo. Sin embargo, este avance también ha generado nuevos desafíos en materia de seguridad digital, especialmente en comunidades con poca formación en ciberseguridad. En Nicaragua, muchas personas desconocen los riesgos asociados al entorno digital, lo que los hace vulnerables a fraudes, robo de identidad y otras amenazas cibernéticas. Esta situación es aún más crítica en zonas rurales y semiurbanas como en la comunidad de Monte Fresco, Villa El Carmen, donde el acceso a educación en seguridad informática es limitado.

Este estudio se alinea con el Plan Nacional de Lucha contra la Pobreza y para el Desarrollo Humano del Gobierno de Nicaragua (Nicaragua, 2022), ya que busca fortalecer la alfabetización digital en la comunidad, promoviendo el acceso equitativo a la educación y reduciendo la brecha tecnológica. La seguridad digital es un pilar esencial para el desarrollo sostenible, pues permite que personas y negocios locales operen en entornos digitales de manera segura, fomentando así la inclusión y el crecimiento económico (ONU, 2021).

El desarrollo de este prototipo educativo en ciberseguridad responde a la necesidad de capacitar a la comunidad en prácticas de protección digital. Este prototipo no solo facilitará el acceso a información relevante de manera didáctica e interactiva, sino que también contribuirá a la generación de habilidades tecnológicas esenciales en la población. Al fortalecer la seguridad digital, se promoverá una mayor confianza en el uso de tecnologías, lo que puede traducirse en

nuevas oportunidades económicas y sociales para la comunidad (Flores, M., & Martínez, R., 2020).

Desde una perspectiva científica, este estudio aporta al campo de la ingeniería en sistemas al diseñar y evaluar un modelo educativo basado en tecnologías interactivas para la enseñanza de ciberseguridad. Además, puede servir como referencia para futuros proyectos de capacitación digital en comunidades con características similares, contribuyendo así al avance del conocimiento en educación tecnológica.

Los principales beneficiarios de este proyecto son los habitantes de Monte Fresco, quienes adquirirán conocimientos esenciales para proteger su información en entornos digitales. De manera indirecta, también se beneficiarán instituciones educativas y organizaciones comunitarias, ya que podrán replicar el modelo en otras zonas vulnerables, ampliando el impacto del estudio.

En términos de impacto social, este estudio contribuye a la reducción de la brecha digital, promoviendo el acceso equitativo a la educación en ciberseguridad y mejorando la seguridad en el uso de tecnologías en sectores desprotegidos. Esto no solo fortalece la resiliencia digital de la comunidad, sino que también sienta las bases para su integración en la economía digital, reduciendo los riesgos de exclusión tecnológica y potenciando el desarrollo humano sostenible.

5.5. Limitaciones

El desarrollo del prototipo de una plataforma de aprendizaje en ciberseguridad en la comunidad de Monte fresco, Villa el Carmen basada en Canvas LMS, enfrentó diversas limitaciones que influyeron en su planificación y posibles aplicaciones futuras. Uno de los principales desafíos fue la infraestructura tecnológica en Monte Fresco, donde el acceso a internet es inestable y muchas personas no cuentan con dispositivos adecuados. Esto limitó la viabilidad de una plataforma completamente en línea, lo que llevó a considerar estrategias alternativas, como el acceso a materiales descargables y el uso de recursos que puedan funcionar sin conexión permanente.

Otra barrera importante fue la falta de conocimiento en ciberseguridad dentro de la comunidad. Durante la recopilación de datos mediante entrevistas semiestructuradas, se identificó que muchas personas no eran conscientes de los riesgos digitales ni de la importancia de proteger su información en línea. Esta situación dificultó la obtención de información detallada sobre sus necesidades específicas. Para abordar esta limitación, se implementaron preguntas adaptadas y ejemplos prácticos que facilitaran la comprensión de los conceptos clave, permitiendo así una mejor identificación de los aspectos a reforzar en la plataforma.

Además, las restricciones económicas representaron un obstáculo significativo. La falta de financiamiento limitó la integración de herramientas avanzadas dentro de Canvas LMS y la posibilidad de realizar pruebas piloto con usuarios de la comunidad. Esto resaltó la importancia de establecer alianzas estratégicas con instituciones educativas, organizaciones tecnológicas y entidades gubernamentales que puedan aportar recursos para la implementación y mejora del prototipo en el futuro.

Otro aspecto clave fue la sostenibilidad del prototipo a largo plazo. Al no haber sido implementado, quedó pendiente la planificación de su mantenimiento, actualización y posible expansión a otras comunidades. Para garantizar su continuidad, sería necesario capacitar a futuros administradores del sistema y desarrollar materiales de apoyo que permitan su uso de manera autónoma. Esto facilitaría que la comunidad pueda apropiarse de la plataforma y seguir beneficiándose de su contenido con el tiempo.

A pesar de estas limitaciones, el desarrollo del prototipo permitió obtener información valiosa sobre los desafíos de llevar educación en ciberseguridad a comunidades con acceso restringido a la tecnología. Este aprendizaje no solo servirá para mejorar la plataforma, sino que también podrá aplicarse en futuros proyectos con objetivos similares, contribuyendo a reducir la brecha digital y fortalecer la seguridad en línea en entornos vulnerables.

5.6. Supuestos Básicos

La comunidad de Monte Fresco carece de conocimientos básicos en ciberseguridad, según estudios previos y datos recopilados en la fase inicial del proyecto, lo que indica una falta de formación en esta área crucial para la protección de información personal y comunitaria. Esta carencia de conocimientos expone a los miembros de la comunidad a riesgos significativos, como el robo de identidad y fraudes en línea. Para abordar esta necesidad, se diseñará un prototipo educativo que será accesible y usable por todos los miembros de la comunidad, independientemente de su nivel de alfabetización digital. La validación del prototipo con un grupo piloto representativo asegurará que el diseño sea adecuado y efectivo para la comunidad, permitiendo ajustes basados en retroalimentación directa. La implementación del prototipo no solo mejorará los conocimientos y prácticas de ciberseguridad de los participantes, sino que también fomentará una cultura de seguridad digital en la comunidad. Este impacto se medirá a través de evaluaciones pre y post en la prueba del prototipo, proporcionando datos concretos sobre la mejora en los conocimientos y prácticas de ciberseguridad de los participantes.

5.7. Categorías, temas y patrones emergentes de la investigación

5.7.1. Categorías

En la investigación se identificaron tres categorías fundamentales. La primera es ciberseguridad y educación digital, que abarca la necesidad de formación en ciberseguridad, la alfabetización digital y las amenazas cibernéticas que afectan a comunidades vulnerables. En Monte Fresco, la falta de conocimientos en estos temas aumenta el riesgo de sufrir fraudes electrónicos, robo de identidad y otros ataques digitales. Esto hace evidente la necesidad de capacitar a la población en prácticas seguras para navegar en internet.

La segunda categoría es la integración y desarrollo del prototipo educativo, enfocado en la creación de una plataforma accesible y efectiva para la enseñanza de ciberseguridad. Se utilizó Canvas LMS como base del sistema, incorporando elementos de gamificación y aprendizaje intuitivo para facilitar la comprensión de los contenidos. Sin embargo, surgieron desafíos relacionados con la accesibilidad y usabilidad, pues la conectividad limitada y el acceso desigual a dispositivos electrónicos podrían dificultar su implementación.

Otra categoría clave es el impacto social y comunitario, que se centra en cómo la vulnerabilidad digital de Monte Fresco afecta a sus habitantes y en la importancia de su participación en iniciativas de seguridad digital. La falta de formación en ciberseguridad limita no solo la seguridad personal en línea, sino también el desarrollo económico y social de la comunidad. Además, la colaboración con instituciones educativas y gubernamentales es fundamental para garantizar la sostenibilidad y el éxito de la iniciativa a largo plazo.

5.7.2. Temas

Se identificaron varios temas en la formación en ciberseguridad dentro de comunidades semiurbanas. Uno de ellos es la brecha digital, la cual limita el acceso a recursos tecnológicos y a oportunidades de capacitación en seguridad digital. La falta de programas educativos accesibles dificulta la adquisición de conocimientos esenciales para la protección en línea, lo que aumenta la vulnerabilidad ante amenazas cibernéticas.

Otro tema es la adopción de tecnologías y plataformas interactivas para el aprendizaje. La implementación de herramientas como Canvas LMS y la gamificación ha demostrado ser una estrategia efectiva para fortalecer la enseñanza. Sin embargo, su aceptación depende del nivel

de familiaridad de los usuarios con entornos digitales, lo que resalta la necesidad de capacitaciones previas en el uso básico de la plataforma.

Asimismo, la sostenibilidad del proyecto educativo en ciberseguridad es un factor determinante para su impacto a largo plazo. Para garantizar su continuidad, se requiere el establecimiento de estrategias de mantenimiento y actualización constante. Esto incluye el desarrollo de materiales complementarios, como manuales de usuario, y la capacitación de líderes comunitarios que faciliten la implementación y apropiación de la plataforma.

5.7.3. *Patrones Emergentes*

Se identificaron varios patrones emergentes relacionados con la seguridad digital en la comunidad. Uno de los más relevantes fue la relación entre la falta de alfabetización digital y la vulnerabilidad a ciberataques. La ausencia de conocimientos sobre amenazas en línea impidió la adopción de medidas básicas de seguridad, lo que expuso a muchas personas a riesgos cibernéticos.

Otro patrón emergente fue la efectividad de la educación interactiva en la adopción de prácticas seguras. Los modelos de aprendizaje que integraron actividades dinámicas y elementos lúdicos facilitaron la comprensión de los conceptos de ciberseguridad, haciéndolos más accesibles y atractivos.

Asimismo, se identificó que el acceso limitado a tecnología y conectividad constituyó una barrera importante. En comunidades como Monte Fresco, la falta de dispositivos adecuados y la inestabilidad del acceso a internet dificultaron la implementación de herramientas digitales. Para mitigar esta limitación, surgió la necesidad de emplear soluciones híbridas que combinaran material en línea con recursos offline.

Finalmente, otro patrón relevante fue la importancia del enfoque participativo en la aceptación del prototipo. La involucración de la comunidad desde las primeras etapas del proyecto favoreció la apropiación de la herramienta. Además, se observó que el desarrollo de un manual de usuario mejoró la accesibilidad, ya que proporcionó una guía clara para su uso, facilitando su integración en la comunidad.

Estos patrones emergentes resaltaron la necesidad de desarrollar estrategias educativas accesibles y sostenibles, adaptadas a las capacidades tecnológicas y a las necesidades específicas de comunidades con baja alfabetización digital.

6. Perspectiva Teórica

6.1. Estado del Arte

La ciberseguridad se ha convertido en un área prioritaria a nivel global debido al incremento exponencial de amenazas cibernéticas, como el phishing, el malware y el robo de datos. En este contexto, la educación en ciberseguridad ha ganado relevancia como una estrategia clave para mitigar riesgos, especialmente en comunidades vulnerables y con acceso limitado a la tecnología.

A nivel internacional, diversas iniciativas han demostrado el impacto positivo de sistemas educativos interactivos en el aprendizaje de ciberseguridad. Por ejemplo, plataformas como "cyberwise" en Estados Unidos y "cibercafé Toolkit" en Europa han implementado enfoques adaptativos y gamificados para mejorar la comprensión de conceptos básicos de ciberseguridad entre jóvenes y adultos con poca alfabetización digital. Estas herramientas destacan por su

accesibilidad, diseño intuitivo y contenidos localizados que responden a las necesidades específicas de sus usuarios.

En el contexto latinoamericano, países como Colombia y México han avanzado en la creación de programas educativos para comunidades rurales. En Colombia, el proyecto "Ciberseguridad Rural" utilizó tecnologías offline para llevar conocimientos básicos a regiones con poca conectividad, mientras que en México, "ciberseguros" combinó capacitaciones presenciales y digitales para empoderar a comunidades indígenas. Estas experiencias subrayan la importancia de diseñar sistemas híbridos que superen barreras tecnológicas y culturales.

En Nicaragua, los esfuerzos recientes en ciberseguridad han sido liderados por instituciones como el Instituto Nacional Tecnológico (INATEC) y la Universidad Americana (UAM). INATEC ha inaugurado laboratorios especializados en ciberseguridad, como el del Centro Tecnológico Manuel Olivares Rodríguez, con el objetivo de formar técnicos y docentes en esta área. Por su parte, la colaboración entre Fortinet y la UAM ha permitido ofrecer certificaciones internacionales en ciberseguridad, contribuyendo al desarrollo de profesionales competentes en el país. Sin embargo, estas iniciativas se han enfocado principalmente en entornos urbanos, dejando una brecha en comunidades rurales o semiurbanas como Monte Fresco.

Además, el uso de metodologías innovadoras como la gamificación ha demostrado ser efectivo en la enseñanza de ciberseguridad. Estudios han indicado que plataformas interactivas con dinámicas de juego mejoran la retención del conocimiento y fomentan una mayor participación de los usuarios. Por ejemplo, iniciativas como "CyberPatriot" en Estados Unidos han demostrado que los estudiantes que participan en entornos de aprendizaje gamificados desarrollan habilidades críticas en seguridad digital con mayor rapidez y compromiso.

Otro aspecto relevante es la importancia de la accesibilidad tecnológica en comunidades con conectividad limitada. La UNESCO (2023) destaca la necesidad de desarrollar plataformas

educativas que puedan operar en entornos offline o con infraestructura mínima, garantizando que el acceso a la educación en ciberseguridad no dependa exclusivamente de la conectividad a Internet. Este enfoque ha sido adoptado en diversas iniciativas en África y Asia, donde los recursos digitales se distribuyen a través de dispositivos precargados y redes locales para ampliar el acceso a la educación.

Asimismo, investigaciones recientes han resaltado la relevancia de la ciberseguridad en el ámbito educativo, promoviendo políticas gubernamentales y programas de formación obligatorios para docentes y estudiantes. En países como España y Chile, se han implementado marcos normativos que exigen la enseñanza de ciberseguridad en los planes de estudio de educación primaria y secundaria. Estos esfuerzos han generado un impacto positivo en la reducción de vulnerabilidades digitales en menores de edad y en la adopción de buenas prácticas de seguridad digital desde una edad temprana.

Otro elemento clave es la colaboración entre sectores público y privado en el fortalecimiento de la educación en ciberseguridad. Empresas tecnológicas como Microsoft y Google han lanzado iniciativas globales para fomentar la alfabetización digital y la seguridad en línea, brindando acceso a cursos gratuitos y herramientas de protección para estudiantes y docentes. Estas alianzas estratégicas han permitido ampliar el alcance de los programas educativos y garantizar que más personas puedan acceder a formación en ciberseguridad sin restricciones económicas o geográficas.

Estas experiencias, tanto internacionales como locales, proporcionan un marco de referencia valioso para el desarrollo de una plataforma educativa en ciberseguridad dirigida a Monte Fresco. Integrar elementos como la gamificación, la accesibilidad offline y un enfoque pedagógico adaptativo puede asegurar la relevancia y efectividad del prototipo.

6.2. Perspectiva Teórica Asumida

La perspectiva teórica asumida en este proyecto se basa en varios enfoques y teorías que subrayan la importancia de la educación en ciberseguridad y la alfabetización digital en comunidades vulnerables. A continuación, se detallan los principales componentes teóricos que sustentan esta investigación:

6.2.1. Teoría del Aprendizaje Constructivista

El constructivismo, propuesto por teóricos como Jean Piaget y Lev Vygotsky, sostiene que el aprendizaje es un proceso activo en el cual los individuos construyen nuevos conocimientos a partir de sus experiencias previas. En el contexto de la ciberseguridad, esta teoría sugiere que los miembros de la comunidad de Monte Fresco aprenderán mejor si pueden relacionar los nuevos conceptos de ciberseguridad con sus experiencias cotidianas. Por lo tanto, el prototipo educativo debe ser diseñado de manera que los contenidos sean relevantes y contextualizados, permitiendo a los participantes construir su comprensión de la ciberseguridad de manera significativa (Piaget, 1952) (Vygotsky, 1978).

6.2.2. Teoría del Capital Social

La teoría del capital social, desarrollada por autores como Pierre Bourdieu y Robert Putnam, enfatiza la importancia de las redes sociales y las relaciones comunitarias en la difusión de conocimientos y prácticas. En Monte Fresco, la cooperación y el apoyo comunitario son valores culturales importantes que pueden facilitar la implementación del programa educativo en ciberseguridad. Al involucrar a líderes comunitarios y fomentar la colaboración entre los miembros de la comunidad, se puede aprovechar el capital social existente para promover la

adopción de prácticas de ciberseguridad y fortalecer la resiliencia comunitaria frente a amenazas digitales (Putnam, 2000) (Bourdieu, 1986).

6.2.3. Teoría de la Alfabetización Digital

La alfabetización digital es un concepto que abarca no solo la capacidad de usar tecnologías digitales, sino también la comprensión crítica de los riesgos y oportunidades asociados con su uso. Según (Gilster, 1997), la alfabetización digital implica habilidades como la navegación en internet, la evaluación de la información en línea y la protección de la privacidad digital. En el contexto de Monte Fresco, la alfabetización digital es fundamental para empoderar a los miembros de la comunidad y reducir su vulnerabilidad a amenazas cibernéticas. El prototipo educativo debe abordar tanto las habilidades técnicas como la conciencia crítica sobre la ciberseguridad.

6.2.4. Enfoque Participativo

El enfoque participativo en el diseño de sistemas educativos es crucial para garantizar su aceptación y efectividad. Según (Flores, M., & Martínez, R., 2020), involucrar a los usuarios finales en la identificación de necesidades y en la validación de prototipos asegura que las soluciones sean culturalmente relevantes y técnicamente apropiadas. En Monte Fresco, donde las barreras culturales y tecnológicas pueden limitar la adopción de nuevas herramientas, es esencial que los miembros de la comunidad participen activamente en el desarrollo y la implementación del prototipo educativo. Esto no solo mejora la relevancia del contenido, sino que también fomenta un sentido de propiedad y compromiso con el proyecto.

6.2.5. Teoría de la Gamificación

La gamificación, o el uso de elementos de juego en contextos no lúdicos, ha demostrado ser efectiva en la educación para aumentar la motivación y el compromiso de los estudiantes. Según (Singh, A., & Smith, J., 2021), las plataformas de aprendizaje que incorporan interactividad, gamificación y personalización maximizan el compromiso del usuario. En el prototipo educativo para Monte Fresco, la gamificación puede ser utilizada para hacer que el aprendizaje de la ciberseguridad sea más atractivo y accesible, especialmente para aquellos con baja alfabetización digital. Elementos como recompensas, niveles y desafíos pueden incentivar la participación y facilitar la retención de conocimientos.

6.2.6. Integración de las Perspectivas Teóricas

La integración de estas perspectivas teóricas proporciona una base sólida para el diseño y la implementación del prototipo educativo en ciberseguridad. Al combinar el constructivismo, el capital social, la alfabetización digital, el enfoque participativo y la gamificación, se puede desarrollar una herramienta educativa que no solo mejore los conocimientos y prácticas de ciberseguridad de los participantes, sino que también fortalezca la resiliencia comunitaria y promueva una cultura de seguridad digital en Monte Fresco.

7. Metodología

7.1. Enfoque cualitativo asumido y su justificación

El estudio que se realizó adoptó un enfoque cualitativo, ya que se consideró la mejor opción para comprender en profundidad las necesidades de formación en ciberseguridad de la comunidad de Monte Fresco. Este enfoque permitió analizar las percepciones, conocimientos y experiencias de los participantes en relación con la seguridad digital en su contexto real, lo cual resultó relevante para identificar las condiciones de alfabetización digital y seguridad en línea en la comunidad.

Asimismo, el estudio tuvo un carácter prospectivo, transversal y exploratorio. Fue prospectivo porque no solo describió la situación actual de la comunidad en términos de ciberseguridad, sino que también proporcionó información útil para el desarrollo de estrategias futuras. Se clasificó como transversal porque la recopilación de datos se realizó en un solo momento sin un seguimiento a largo plazo, lo que permitió obtener una imagen clara de la realidad en un punto específico en el tiempo. Además, se consideró exploratorio debido a la falta de estudios previos sobre la alfabetización en ciberseguridad en Monte Fresco, lo que facilitó la identificación de brechas en el conocimiento y proporcionó datos clave para el diseño de estrategias educativas adaptadas a las necesidades de la comunidad.

7.2. Muestra Teórica y Sujetos del Estudio

7.3. Muestra

La comunidad de Monte Fresco, ubicada en Villa El Carmen, Managua, cuenta con una población de 1,296 habitantes (Instituto Nacional de Información de Desarrollo [INIDE], 2005). Para esta investigación, se utilizó un muestreo teórico compuesto por cuatro participantes, seleccionados bajo criterios, género, ocupación y nivel de alfabetización digital.

7.3.1. Sujeto de estudio

Los sujetos del estudio incluyen miembros de la comunidad de Monte Fresco, quienes aportaron información clave sobre sus prácticas digitales y conocimientos en ciberseguridad. Entre los participantes, se entrevistó al líder comunitario del Consejo del Poder Ciudadano (CPC), quien brindó una perspectiva general sobre el acceso a tecnologías y los desafíos en seguridad digital que enfrenta la comunidad. Además, se seleccionaron tres habitantes de género masculino adicionales con diferentes niveles de experiencia en el uso de tecnologías digitales, desde principiantes hasta usuarios con mayor familiaridad con herramientas tecnológicas. Esto permitió obtener una visión integral de las necesidades y desafíos en ciberseguridad dentro de la comunidad.

La selección de la muestra y la metodología empleada garantizan que los hallazgos sean representativos de la problemática estudiada, a pesar de no basarse en un muestreo probabilístico.

7.4. Métodos y Técnicas de Recolección de Datos

7.4.1. Método

El presente estudio adoptó un enfoque cualitativo, ya que su objetivo fue explorar en profundidad las percepciones, conocimientos y necesidades de formación en ciberseguridad dentro de la comunidad de Monte Fresco. Este enfoque se consideró el más adecuado porque permite analizar fenómenos en su contexto natural, capturando experiencias subjetivas y dinámicas sociales que no podrían ser abordadas con métodos cuantitativos.

El enfoque cualitativo permitió analizar a profundidad las percepciones y conocimientos de los participantes, facilitando la identificación de patrones y necesidades específicas para el diseño del prototipo educativo en ciberseguridad basado en Canvas LMS.

7.4.2. Técnica

Para la recolección de datos, se aplicaron entrevistas semiestructuradas, una técnica que permitió obtener respuestas profundas y flexibles, adaptando la conversación a las experiencias individuales de los entrevistados.

La recopilación de información se llevó a cabo mediante entrevistas semiestructuradas, aplicadas a un grupo de cuatro participantes, seleccionados en función de criterios como edad, género, ocupación y nivel de alfabetización digital. Entre ellos, se incluyó al líder comunitario del Consejo del Poder Ciudadano (CPC), quien proporcionó una visión general sobre el acceso a la tecnología y los principales desafíos en materia de ciberseguridad dentro de la comunidad.

Las entrevistas fueron diseñadas con un guion de preguntas abiertas, abarcando aspectos clave como:

- Experiencia en el uso de tecnología dentro de la comunidad.
- Percepción de riesgos cibernéticos, incluyendo fraudes en línea, malware y robo de identidad.
- Conocimientos previos en ciberseguridad y hábitos digitales.

- Interés en recibir formación en seguridad digital y métodos de aprendizaje preferidos.

Cada entrevista tuvo una duración de 15 a 20 minutos y se realizó en un entorno accesible y cómodo para los participantes. Con el consentimiento informado de los entrevistados, las sesiones fueron grabadas con el propósito de garantizar una transcripción precisa y un análisis detallado de los datos. (ver anexo, Figura: 7,8,9)

7.5. Criterios de Calidad Aplicados: Credibilidad, Confiabilidad y Triangulación

7.5.1. Credibilidad

La credibilidad se fundamentó en la evaluación de los instrumentos aplicados para determinar si permitían obtener información precisa sobre la alfabetización digital y los desafíos de ciberseguridad en la comunidad de Monte Fresco. Se verificó que los métodos empleados estuvieran alineados con los objetivos del estudio y fueran adecuados para reflejar la realidad investigada. La coherencia entre los datos obtenidos y la problemática planteada permitió asegurar que los resultados fueran representativos.

7.5.2. Confiabilidad

En el proceso de la técnica de la entrevista semiestructurada, con el consentimiento de los participantes, cada sesión fue grabada para garantizar la fidelidad de la información.

Se garantizó en todo momento la confidencialidad de la información recopilada, protegiendo la identidad de los participantes y asegurando que los datos obtenidos fueran utilizados exclusivamente para fines académicos. Las grabaciones fueron almacenadas en un

entorno seguro una vez concluido el análisis, en cumplimiento con principios éticos de investigación cualitativa.

7.5.3. Triangulación

La triangulación se realizó mediante la comparación de la información recopilada con diversas fuentes, incluyendo literatura académica y antecedentes sobre alfabetización digital y ciberseguridad en comunidades con acceso limitado a tecnologías. Esta técnica permitió validar los hallazgos al contrastarlos con marcos teóricos preexistentes, asegurando que las conclusiones estuvieran fundamentadas en múltiples perspectivas y reflejaran con precisión la realidad investigada.

7.6. Métodos y Técnicas para el Procesamiento de Datos y Análisis de Información

El procesamiento de datos en esta investigación se realizó mediante métodos cualitativos, con el propósito de organizar y analizar la información de manera estructurada. Para ello, se empleó una Matriz de Reducción de Datos, la cual permitió clasificar y presentar la información de forma clara, facilitando su interpretación (*ver Anexo, Tabla 1*).

La Matriz de Reducción de Datos facilitó el análisis de los resultados obtenidos, permitiendo identificar tendencias y resumir la información clave relacionada con el uso de tecnología, el nivel de conocimiento en ciberseguridad y los principales riesgos percibidos por la comunidad. A partir de esta matriz, se destacaron los siguientes hallazgos:

Uso de tecnología. Se determinó que el 90% de la población utiliza dispositivos móviles, principalmente celulares y tablets, incluyendo niños desde los 8 años.

Conocimiento en ciberseguridad. Se evidenció una baja comprensión sobre amenazas digitales como phishing y malware, aunque algunos participantes mostraron cierto conocimiento sobre estafas en redes sociales.

Principales riesgos identificados. Los participantes destacaron que la adicción a pantallas y el ciberacoso son los problemas más comunes entre jóvenes y niños.

Interés en capacitaciones. Se identificó un alto interés en recibir formación en ciberseguridad, con preferencia por materiales audiovisuales como videos y simulaciones.

Acceso a internet. La mayoría de los habitantes accede a internet mediante datos móviles en lugar de redes WiFi, lo que puede influir en el diseño de estrategias educativas digitales.

Los resultados detallados de este análisis se presentan en la Matriz de Reducción de Datos (*ver Anexo, Tabla 1*).

8. Discusión de hallazgos y resultados

8.1. Necesidades de Formación en Ciberseguridad

Durante la investigación se realizaron entrevistas con los habitantes de la comunidad Monte Fresco para evaluar su conocimiento y percepción sobre la seguridad digital. Los resultados mostraron que una gran parte de la comunidad ha escuchado sobre estafas digitales y reconoce la importancia de proteger su información en línea. Sin embargo, se identificó un desconocimiento significativo sobre los riesgos del uso inadecuado de dispositivos móviles y plataformas digitales, así como la falta de capacitación formal en tecnologías de seguridad.

Un hallazgo clave fue que, aunque los hogares cuentan con dispositivos como celulares y computadoras, la mayoría de los encuestados no ha recibido capacitaciones sobre el uso seguro de la tecnología. Además, muchos desconocen técnicas básicas para proteger su información, como la identificación de estafas en línea (phishing) o la utilización de software de seguridad.

8.2. Integración del Prototipo de la Plataforma

Se realizó la integración del prototipo de la interfaz, asegurando que cumpliera con los elementos esenciales de aprendizaje para los tres roles definidos: administrador, docente y estudiante. La estructura de la plataforma se integró para garantizar una experiencia de usuario intuitiva y eficiente, permitiendo la gestión y acceso a los contenidos educativos de manera organizada. (*ver Anexo, Figura 4, Figura 5, Figura 6*).

8.3. Incorporación de contenido interactivo y adaptado.

Para mejorar el aprendizaje, la comunidad expresó su preferencia por materiales educativos interactivos. Se destacó el uso de cuestionarios, simulaciones y ejemplos prácticos como estrategias clave para facilitar la comprensión y retención del conocimiento en temas de ciberseguridad.

La investigación también reveló que existe un interés por aprender sobre protección de información digital, especialmente en la identificación de fraudes y malware. Esto justifica la incorporación de módulos específicos dentro de la plataforma que cubran estos temas con ejemplos reales y ejercicios prácticos.

8.4. Resultados finales.

Los hallazgos de la investigación muestran una necesidad clara de formación en ciberseguridad dentro de la comunidad de Monte Fresco. A pesar de la presencia de dispositivos tecnológicos en los hogares, la falta de educación en seguridad digital deja a los usuarios vulnerables a diversas amenazas.

La propuesta de una plataforma de aprendizaje en línea enfocada en la ciberseguridad puede ayudar a cerrar esta brecha, proporcionando contenido accesible, interactivo y adaptado a las condiciones tecnológicas de la comunidad. La investigación reafirma la importancia de desarrollar soluciones educativas que no solo transmitan información, sino que también fomenten la participación activa y la aplicación práctica de los conocimientos adquiridos.

8.5. Recomendaciones

Aunque no se implementó la plataforma, la información obtenida sirvió como base para estructurar su diseño y funcionalidad, asegurando que estuviera alineada con las características y el nivel de alfabetización digital de la comunidad.

Como parte de la implementación del sistema, se recomienda la elaboración de un manual de usuario dirigido a los administradores, docentes y estudiantes. Este manual debe incluir instrucciones detalladas sobre el uso de la plataforma, desde la gestión de usuarios hasta la navegación en los contenidos educativos y la realización de actividades interactivas.

Asimismo, el contenido educativo de este prototipo está enfocado en jóvenes y adultos, adaptando los materiales a sus necesidades y niveles de comprensión tecnológica. Esto garantizará que los conocimientos impartidos sean aplicables y útiles en su vida diaria, fortaleciendo la seguridad digital de la comunidad.

9. Referencias

- BID, B. I. (2023). Obtenido de Banco Interamericano de Desarrollo: <https://www.iadb.org>
- Bourdieu, P. (1986). *The forms of capital*. Greenwood.
- Flores, M., & Martínez, R. (2020). *Alfabetización digital y ciberseguridad en comunidades vulnerables*. Editorial Académica Española.
- Fortinet. (2023). Obtenido de <https://fortinet.com>
- Gilster, P. (1997). *Digital literacy*. Wiley Computer Publishing.
- INATEC, I. N. (2023). Obtenido de <https://inatec.gob.ni>
- Nica, E. D. (2023). *El Diario Nica*. Obtenido de <https://www.eldiarionica.com>
- Nicaragua, G. d. (2022). *Desarrollo Humano del Gobierno de Nicaragua*. Gobierno de Nicaragua.
- ONU, O. d. (2021). *Informe sobre brecha digital y seguridad cibernética en América Latina*. Obtenido de <https://www.un.org>
- Piaget, J. (1952). *The origins of intelligence in children*. W. W. Norton.
- Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. Simon & Schuster.
- Singh, A., & Smith, J. (2021). Gamification in education: Enhancing learning experiences. *Educational Research Journal*, 35(2), 112-130.
- UAM, U. A. (2023). Obtenido de <https://uam.edu.ni>
- Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

10. Anexos o Apéndices

Diseño del sistema informático

1. Estructura y Diseño de la Plataforma

En esta sección se presenta la guía, diseño y estructura del demo de la plataforma de aprendizaje en ciberseguridad, desarrollado con Canvas LMS para la comunidad de Monte Fresco, Villa El Carmen, Managua, Nicaragua. El prototipo fue diseñado con el objetivo de capacitar a los habitantes en buenas prácticas de seguridad digital, proporcionando una herramienta educativa accesible y estructurada. Este desarrollo se alinea con los objetivos de crear una interfaz intuitiva para los roles de administrador, profesor y estudiante, así como de implementar módulos educativos enfocados en phishing y malware.

El desarrollo del demo responde a la necesidad de ofrecer un entorno accesible y estructurado donde los usuarios puedan interactuar de manera eficiente. La elección de Canvas LMS se fundamenta en su flexibilidad, facilidad de uso y capacidad para adaptarse a diversos contextos educativos. Gracias a su interfaz intuitiva, la plataforma facilita la gestión de cursos, la entrega de contenidos y la evaluación de los participantes, cumpliendo con el objetivo de desarrollar un prototipo basado en una herramienta robusta y de fácil adopción.

El apartado describe en detalle el funcionamiento de la plataforma, los roles asignados a los usuarios, la metodología empleada para el diseño del demo y la estructura de los módulos que conforman el curso piloto. Estos módulos, enfocados en phishing y malware, están diseñados para brindar una experiencia de aprendizaje clara y efectiva. Además, se proporcionan recomendaciones para optimizar y facilitar la futura implementación de la plataforma en un entorno de producción, asegurando que cumpla con los objetivos de ser una herramienta educativa accesible y de alto impacto para la comunidad de Monte Fresco.

2. Definición de Requerimientos

Para garantizar la funcionalidad de la plataforma, se establecen los siguientes requerimientos:

a. Requerimientos Funcionales y No Funcionales

- Implementación de módulos de aprendizaje interactivos.
- Gestión de usuarios con roles definidos.
- Seguridad y privacidad de datos.
- Compatibilidad con dispositivos móviles.
- Accesibilidad y facilidad de navegación.

3. Metodología del Desarrollo

a. Tipo de Metodología

Para el desarrollo del demo, se adoptó la metodología ágil Scrum, la cual permitió una implementación progresiva y flexible. Este enfoque facilitó la entrega de funcionalidades en ciclos de desarrollo cortos, optimizando el proceso de pruebas y ajustes en función de la retroalimentación recibida.

b. Diseño de Arquitectura

i. Capa de Entidades

Define la estructura de datos y la relación entre los elementos clave dentro de la plataforma, asegurando que la información fluya de manera eficiente entre los diferentes roles de usuario.

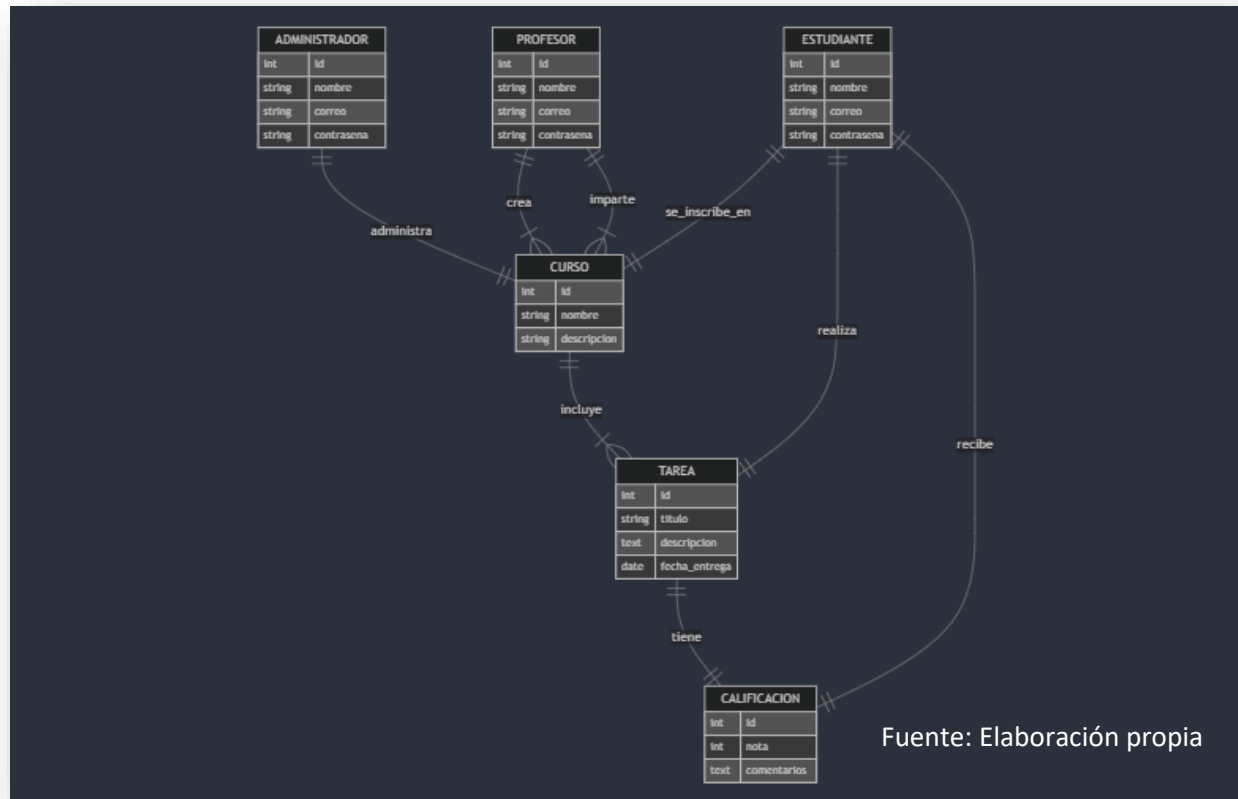
ii. Capa de Datos

Se enfoca en la organización, almacenamiento y gestión de la información dentro del sistema, garantizando la integridad y seguridad de los datos.

4. Diagrama de Entidad-Relación

Se ha diseñado un diagrama de entidad-relación para estructurar la base de datos de la plataforma, asegurando la correcta integración de los roles y funcionalidades dentro de Canvas LMS. En caso de que se aplique para una aplicación móvil, se utilizará un diagrama de clases para definir su estructura.

Figura 1: Diagrama de Entidad-Relación



Entidades y sus responsabilidades y dependencias

- Administrador → Administra Cursos.
- Profesor → Crea e imparte Cursos, los cuales incluyen Tareas.
- Estudiante → Se inscribe en Cursos, realiza Tareas y recibe Calificaciones.
- Tareas → Son parte de los Cursos y generan Calificaciones.

El diagrama de entidades del sistema refleja la estructura de la base de datos y la relación entre sus principales componentes. En este modelo, se identifican entidades como Usuario, Curso,

Módulo, Evaluación y Material Didáctico, cada una con atributos específicos que definen su funcionalidad dentro de la plataforma. La entidad Usuario se subdivide en los roles de Administrador, Profesor y Estudiante, estableciendo permisos diferenciados para cada uno.

Cada curso está compuesto por múltiples módulos, los cuales incluyen materiales didácticos y evaluaciones. Los estudiantes pueden inscribirse en distintos cursos y completar actividades asociadas, mientras que los profesores administran el contenido y el proceso de evaluación. Esta estructura permite un flujo de información organizado, asegurando que los datos de los usuarios y el contenido educativo sean gestionados de manera eficiente dentro de la plataforma.

5. Casos de Uso

Los principales casos de uso identificados para la plataforma incluyen:

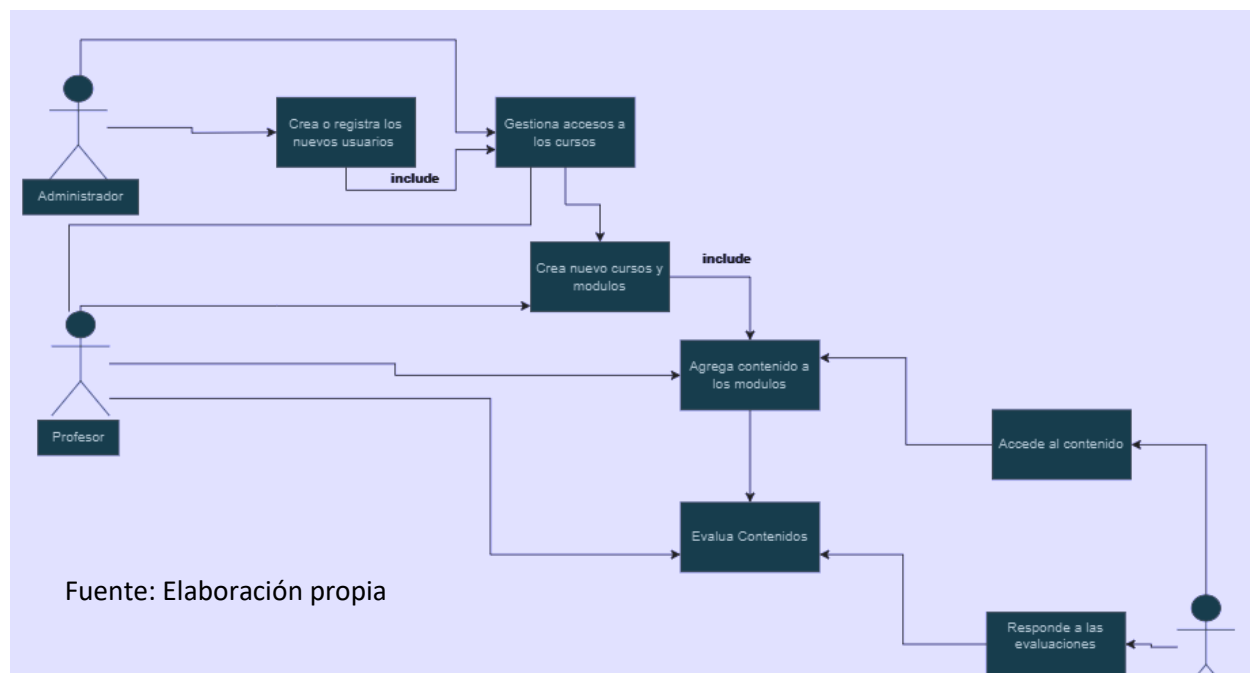
Registro e inicio de sesión de usuarios.

Creación y gestión de cursos por parte de los profesores.

Participación en actividades y evaluaciones por parte de los estudiantes.

Administración y monitoreo de la plataforma por parte de los administradores.

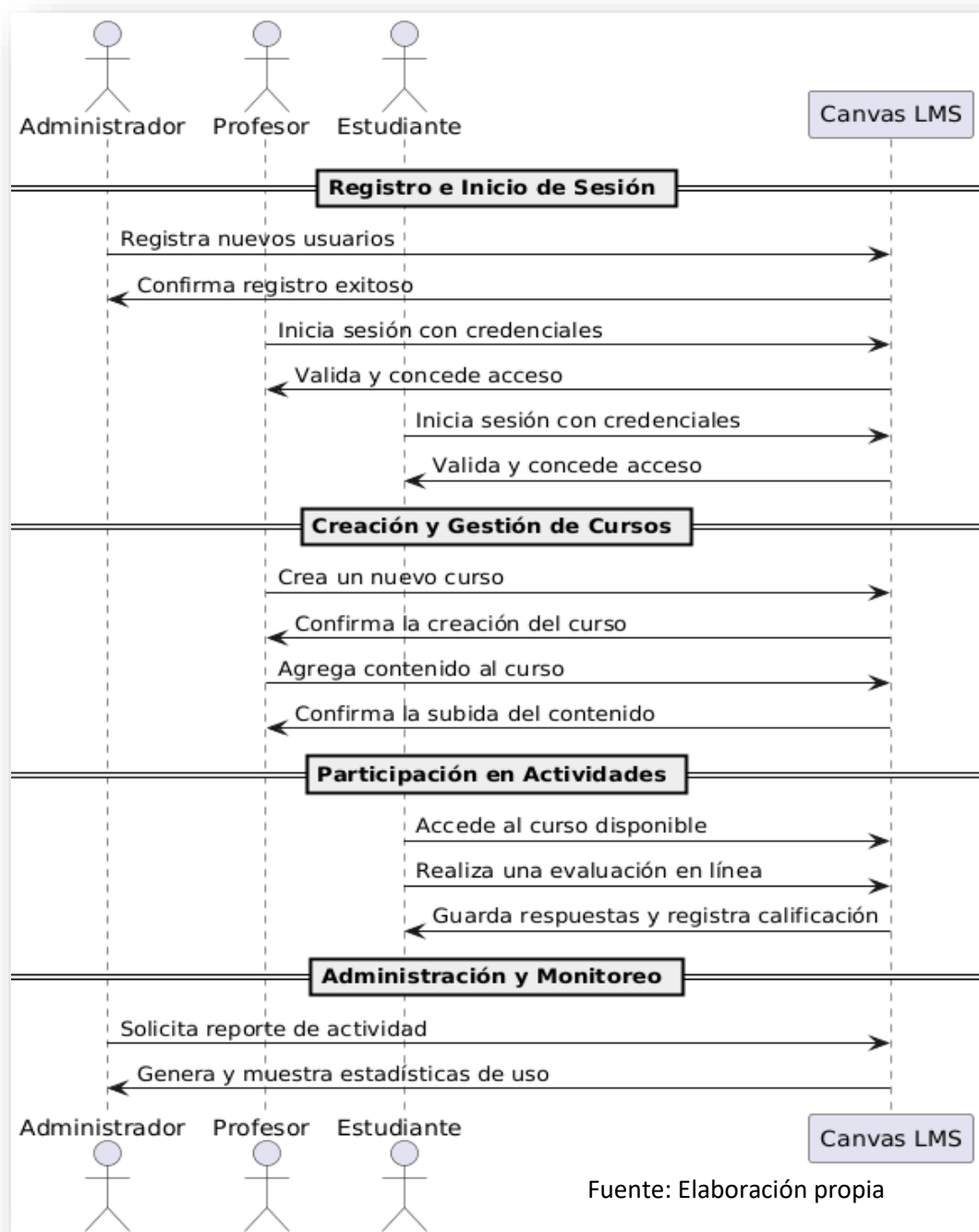
Figura 2: Diagrama de Casos de Uso



6. Diagrama de Secuencia

El diagrama de secuencia define la interacción entre los usuarios y los componentes de la plataforma, asegurando que las funciones se ejecuten de manera lógica y estructurada.

Figura 3: Diagrama de Secuencia



6.1 Registro e Inicio de Sesión

En este proceso, el **Administrador** es responsable de registrar nuevos usuarios en la plataforma. Esto implica ingresar los datos de los usuarios en el sistema para que puedan acceder posteriormente. Una vez que el Administrador completa el registro, **Canvas LMS** envía una confirmación indicando que el usuario ha sido creado correctamente.

Después del registro, los **Profesores** y **Estudiantes** pueden intentar iniciar sesión en la plataforma. Para ello, ingresan sus credenciales en la interfaz de inicio de sesión. **Canvas LMS** recibe estas credenciales y las valida comparándolas con la base de datos. Si las credenciales son correctas, se concede acceso al usuario; de lo contrario, se deniega el ingreso.

Este proceso es fundamental porque asegura que solo los usuarios registrados puedan acceder a la plataforma y desempeñar sus respectivas funciones.

6.2 Creación y Gestión de Cursos

Una vez dentro de la plataforma, los Profesores tienen la capacidad de crear y gestionar cursos. Para ello, inician el proceso de creación de un nuevo curso, enviando la solicitud a Canvas LMS. La plataforma procesa esta solicitud y devuelve una confirmación indicando que el curso ha sido creado con éxito.

Después de la creación del curso, el Profesor puede agregar contenido educativo, como documentos, videos, cuestionarios y evaluaciones. Cada vez que se agrega contenido, Canvas LMS lo almacena y confirma la operación, asegurando que el material está disponible para los estudiantes.

Este proceso es crucial, ya que define la estructura del aprendizaje dentro de la plataforma y permite que los estudiantes accedan a materiales organizados y actualizados por sus profesores.

6.3 Participación en Actividades

Los Estudiantes pueden acceder a los cursos disponibles dentro de Canvas LMS y explorar los módulos de aprendizaje. Una de las principales actividades dentro de un curso es la realización de evaluaciones, donde el estudiante responde preguntas o completa tareas asignadas por el profesor.

Cuando un estudiante realiza una evaluación, la plataforma recibe sus respuestas y procesa la calificación. Dependiendo de la configuración del curso, la calificación puede calcularse automáticamente o requerir la revisión del profesor. Una vez que el puntaje es registrado en el sistema, el estudiante puede visualizar sus resultados y recibir retroalimentación.

Este proceso permite que los estudiantes midan su progreso y mejoren su aprendizaje con base en sus calificaciones y la información proporcionada por los docentes.

6.4 Administración y Monitoreo

Para garantizar el buen funcionamiento de la plataforma y mejorar la experiencia de los usuarios, los Administradores pueden generar informes de actividad dentro de Canvas LMS. Estos informes pueden incluir información sobre la cantidad de usuarios activos, el número de cursos creados, el rendimiento de los estudiantes en las evaluaciones y otros datos relevantes.

Cuando un administrador solicita un reporte, la plataforma analiza la información almacenada y genera un documento con las estadísticas correspondientes. Este reporte se muestra en la interfaz del administrador, quien puede utilizarlo para evaluar el desempeño de la plataforma y tomar decisiones estratégicas para su optimización.

Este proceso es clave para el mantenimiento del sistema, ya que permite a los administradores supervisar el uso de la plataforma y realizar mejoras para garantizar una experiencia de aprendizaje eficiente.

7. Definición del Módulo

Se han diseñado módulos específicos para estructurar el contenido educativo dentro de Canvas LMS, organizados de la siguiente manera:

Modulo 1: Phishing - Conceptos Básicos

- Conceptos básicos.
- Conociendo acerca del Phishing.
- Tareas – Conocimientos Básicos sobre Phishing y Ciberseguridad.
- Phishing: Conociendo la amenaza y aprendiendo a protegernos.

8. Factibilidad Económica

La evaluación del prototipo de la plataforma incluyó un análisis detallado de costos y recursos necesarios para una posible implementación futura. Se consideraron diversas opciones, como la adquisición de servidores físicos, la implementación de una infraestructura cloud o la contratación del servicio de hosting directamente desde la página oficial de Canvas (<https://www.instructure.com/es>). Este análisis permitió concluir que Canvas LMS representa una solución viable debido a su naturaleza de código abierto, lo que minimiza los costos de licencia y ofrece flexibilidad para adaptarse a las necesidades de la comunidad de Monte Fresco. Además, se evaluó que la opción de hosting oficial de Canvas podría simplificar la gestión técnica y garantizar un soporte especializado, aunque implicaría un costo recurrente.

En el caso de optar por una infraestructura cloud, se identificó que esta alternativa permitiría escalabilidad y acceso remoto, facilitando la disponibilidad de la plataforma para los usuarios. Sin embargo, también se consideró que requeriría una inversión inicial en configuración y mantenimiento técnico. Por otro lado, la adquisición de servidores físicos implicaría mayores costos iniciales y de mantenimiento, pero ofrecería un control total sobre la infraestructura. Este

análisis se alineó con los objetivos de diseñar una plataforma accesible, sostenible y de bajo costo para la comunidad.

Además, se llevó a cabo un análisis comparativo entre soluciones comerciales y Canvas LMS, determinando que la inversión inicial se reduciría significativamente al no requerir licencias costosas ni infraestructura compleja. La capacitación de administradores y docentes se planteó como una inversión estratégica a largo plazo, asegurando la sostenibilidad del proyecto sin incurrir en costos adicionales elevados. De esta manera, el prototipo demostró que la plataforma podría mantenerse operativa con un presupuesto accesible y optimizado, cumpliendo con los objetivos de ser una herramienta educativa eficiente y de bajo costo para la comunidad.

Figura 4: Interfaz de Administrador

Configuraciones de Eddy Guzman

Nombre completo: Eddy Guzman
Este nombre será usado por los profesores para las calificaciones.

Nombre de exhibición: Eddy Guzman
Otros verán este nombre en los foros de discusión, mensajes y comentarios.

Nombre clasificable: Guzman, Eddy
Este nombre aparece en las listas clasificables.

Pronombres: Ninguno
Cuando esté habilitado, este pronombre aparecerá luego de su nombre

Idioma: Español (Latinoamérica)

Zona horaria: Hora de montaña (EE. UU. y Canadá)
Ventanas de mantenimiento: 1.º y 3.º Jueves del mes de 0:05 a 2:05 (Jueves desde 7:05 hasta 9:05 UTC)
Siguiente ventana: Jue 6 de mar de 2025 desde 0:05 hasta 2:05
For maintenance window details please see the [release notes](#).

Maneras para contactar

Direcciones de correo electrónico
ichico2330@gmail.c... ★
[+ Dirección de correo electrónico](#)

Otros contactos	Tipo
+ Método de contacto	

[Editar las configuraciones](#)

[Descargar entregas](#)

[Descargar los contenidos del curso](#)

Servicios en línea

Fuente: Elaboración propia

Figura 5: Interfaz de Profesor

https://canvas.instructure.com/courses/11371777/users

CyberSeg > Personas

63 Ver como estudiante

+ Conjunto de grupos

Todos Grupos

Buscar a personas Todos los roles

+ Personas

Nombre	Identificador de inicio de sesión	Identificación del SIS	Sección	Rol	Última actividad	Actividad total
Alexander	allexx05guillen@gmail.com		Ciber Seguridad - Phishing	Profesor	2 de mar en 19:58	15:47
Beatriz Franco	bfranco9320@gmail.com		Ciber Seguridad - Phishing	Estudiante	27 de feb en 21:14	04:41
Eddy Guzman	ichico2330@gmail.com		Ciber Seguridad - Phishing	Profesor	2 de mar en 9:14	06:42:19

Fuente: Elaboración propia

Figura 6: Interfaz de Estudiante

The screenshot displays the 'CyberSeg > Personas' interface. On the left is a dark sidebar with icons for Cuenta, Tablero, Cursos, Calendario, Bandeja de entrada, and Historial. The main content area has a top bar with 'CyberSeg > Personas' and a source note 'Fuente: Elaboración propia'. Below this is a list of navigation links: Página de Inicio, Anuncios, Tareas, Foros de discusión, Calificaciones, and a 'Personas' section with sub-links: Páginas, Archivos, Programa del curso, Evaluaciones, and Módulos. The 'Personas' section is active, showing tabs for 'Todos' and 'Grupos'. Below the tabs is a search bar 'Buscar a personas' and a role filter 'Todos los roles'. A table lists three users:

	Nombre	Sección	Rol
	Alexander	Ciber Seguridad - Phishing	Profesor
	Beatriz Franco	Ciber Seguridad - Phishing	Estudiante
	Eddy Guzman	Ciber Seguridad - Phishing	Profesor

A notification bubble with the number '10' is visible in the bottom right corner of the sidebar.

Tabla 1: Matriz de Reducción de Datos

Resumen de información obtenida en entrevistas sobre ciberseguridad en Monte Fresco.

Categoría	Entrevista 1 (Ciudadano)	Entrevista 2 (Ciudadano)	Entrevista 3 (Ciudadano)	Entrevista 4 (CPC - Representante Comunitario)
Uso de tecnología	Celulares y laptops.	90% usa tecnología; niños desde 8 años.	Usa celular para plataformas educativas.	90% usa celulares, tablets y laptops.
Conocimientos sobre ciberseguridad	Ha escuchado sobre estafas digitales; desconoce phishing y malware.	Pocos están informados, principalmente los adultos.	No conoce phishing ni malware.	Pocos están informados sobre fraudes digitales.
Principales dispositivos usados	Celulares y laptops.	Celulares, tablets y laptops.	Celulares.	Celulares, tablets y laptops.
Acceso a internet	No menciona dificultades.	La mayoría usa datos móviles en vez de WiFi.	Considera el acceso a internet fácil.	La mayoría usa datos móviles en vez de WiFi.
Capacitaciones previas	No ha recibido capacitación.	Solo se tocan temas en la escuela, no hay programas comunitarios.	No ha recibido capacitación.	La policía dio charlas sobre ciberacoso.

Principales riesgos identificados	Falta de conocimientos sobre seguridad digital.	Adicción a pantallas y ciberacoso en jóvenes.	Adicción a pantallas.	Adicción a pantallas en niños y jóvenes.
Interés en capacitaciones	Sí, le gustaría recibir capacitación.	Sí, hay interés en la comunidad.	Sí, le gustaría recibir capacitación.	Sí, considera que la comunidad estaría interesada.
Preferencias sobre la plataforma	Fácil de usar, con manuales y videos de introducción.	Fácil de entender, más información interactiva.	Interactiva, con módulos educativos.	No menciona preferencia específica.
Formato de material educativo preferido	Videos y simulaciones.	Sesiones interactivas.	Lecturas y videos.	No menciona preferencia específica.
Sugerencias para mejorar la enseñanza	Cursos sobre ciberseguridad.	Usar la escuela y redes sociales para talleres.	Implementar cursos comunitarios.	Usar redes sociales y la escuela para capacitaciones.

Tabla 3: presupuesto

Categoría	Concepto	Detalle	Cantidad	Costo Unitario (C\$)	Costo Total (C\$)
Gastos Administrativos	Papelería	Hojas, carpetas, lápices, etc.	10,00	C\$ 20,00	C\$ 200,00
	Servicios	Impresión, fotocopias	10,00	C\$ 5,00	C\$ 50,00
	Uso de Instalaciones	Espacios de trabajo o salas	0,00	C\$ -	C\$ -
	Otros	Permisos legales u otros	0,00	C\$ -	C\$ -
	Subtotal (Administrativo)				C\$ 250,00
Materiales	Equipos de Recolección de Datos	celulares y tabletas	2,00	C\$ 4.000,00	C\$ 8.000,00
	Cuestionarios/Encuestas	Impresión	10,00	C\$ 5,00	C\$ 50,00
	Libros/Referencias	Adquisición de bibliografía	0,00	C\$ -	C\$ -
	Materiales Didácticos	Materiales para talleres	0,00	C\$ -	C\$ -
	Otros	Alquiler de software o herramientas	2,00	C\$ 3.000,00	C\$ 6.000,00
	Subtotal (Materiales)				XXX

Otros Gastos	Transporte	Visitas de campo	2,00	C\$ 80,00	C\$ 160,00
	Alimentación	Para participantes o equipo	2,00	C\$ 120,00	C\$ 240,00
	Publicaciones	Impresión y difusión de resultados	0,00	C\$ -	C\$ -
	Software	Licencias específicas	1,00	C\$ 2.000,00	C\$ 2.000,00
	Subtotal (Otros Gastos)				C\$ 16.950,00
	Total General:				C\$ 16.950,00

Figura 7: Entrevistas semiestructuradas

Universidad Central de Nicaragua
Campus Central
Facultad de Ingeniería en Sistemas
Entrevista dirigida a los Habitantes de la Comunidad Monte Fresco

Fecha: ____/____/2025 **Hora inicio:** _____ **HoraFinal:** _____

Nombre del entrevistado: _____

La presente entrevista tiene como objetivo recopilar información del tema de estudio: "Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, Managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025." para optar de Ingeniero en sistemas. Los datos proporcionados serán tratados con prudencia y serán totalmente confidenciales, dicha investigación ayudara a la investigación para indagar sobre el tema de estudio. De esta recopilación se presentarán los resultados, conclusiones y recomendaciones. De ante mano se agradece la disponibilidad y el apoyo brindado para esta investigación.

I. Identificación de Necesidades de Formación.

¿Ha escuchado hablar sobre las estafas digitales?

¿Sabe que el mal uso de dispositivos móviles o plataformas puede ocasionar el robo de información o dinero?

En su hogar, ¿usan celulares inteligentes, laptops o computadoras de escritorio?

¿En su comunidad han recibido capacitaciones sobre el uso seguro de la tecnología?

¿Ha participado en cursos o talleres sobre cómo proteger su información digital?

¿Le gustaría recibir asesoría o capacitación sobre el uso seguro de dispositivos móviles y computadoras?

Fuente: Elaboración propia

Figura 8: Entrevista Semiestructurada

¿Qué temas considera importantes para proteger su información digital en sus dispositivos?

¿Qué medidas de seguridad utiliza en sus dispositivos móviles y computadoras?

¿Qué tanto conoce sobre estafas en línea (phishing) y programas maliciosos (malware)?

II. Diseño de la Plataforma

¿Qué características considera importantes en una plataforma de aprendizaje en línea?

¿Cuáles serían las principales dificultades que enfrentaría para utilizar una plataforma de ciberseguridad?

¿En qué dispositivos suele acceder a plataformas educativas en línea (computadora, celular, Tablet)?

III. Desarrollo del Prototipo

¿Qué tan fácil o difícil le resulta navegar en plataformas digitales?

¿Qué tipo de herramientas o funcionalidades le gustaría encontrar en la plataforma para facilitar su aprendizaje?

IV. Módulos Educativos

¿Qué aspectos específicos sobre phishing y malware le gustaría aprender?

¿Considera que los ejemplos prácticos y simulaciones ayudarían a su aprendizaje?

¿Por qué?

¿Qué tipo de actividades o materiales educativos (videos, lecturas, cuestionarios) prefiere?

Fuente: Elaboración propia

Figura 9: Entrevista Semiestructurada**V. Manual de Usuario**

¿Prefiere manuales escritos, tutoriales en video o sesiones interactivas para aprender a usar una nueva plataforma?

¿Qué información le gustaría que incluyera un manual de usuario para la plataforma de aprendizaje?

VI. Comentarios Finales

¿Qué otras sugerencias tienen para mejorar la enseñanza de ciberseguridad en su comunidad?

Fuente: Elaboración propia

Figura 10: Resultados de la Entrevista

Universidad Central de Nicaragua
Campus Central
Facultad de Ingeniería en Sistemas
Entrevista dirigida a los Habitantes de la Comunidad Monte Fresco

Fecha: 08/02/2025 Hora inicio: 9:20 Hora Final: _____

Nombre del entrevistado: Jerson Obas Gutierrez Ruiz

La presente entrevista tiene como objetivo recopilar información del tema de estudio: "Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, Managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025." para optar de Ingeniero en sistemas. Los datos proporcionados serán tratados con prudencia y serán totalmente confidenciales, dicha investigación ayudara a la investigación para indagar sobre el tema de estudio. De esta recopilación se presentarán los resultados, conclusiones y recomendaciones. De ante mano se agradece la disponibilidad y el apoyo brindado para esta investigación.

I. Identificación de Necesidades de Formación.

¿Ha escuchado hablar sobre las estafas digitales? Si

¿Sabe que el mal uso de dispositivos móviles o plataformas puede ocasionar el robo de información o dinero? NO SABER

En su hogar, ¿usan celulares inteligentes, laptops o computadoras de escritorio? Si

¿En su comunidad han recibido capacitaciones sobre el uso seguro de la tecnología? NO

¿Ha participado en cursos o talleres sobre cómo proteger su información digital? NUNCA

¿Le gustaría recibir asesoría o capacitación sobre el uso seguro de dispositivos móviles y computadoras? Si

Fuente: Elaboración propia

Figura 11: Resultados de la Entrevista

¿Qué temas considera importantes para proteger su información digital en sus dispositivos? *El uso de las contraseñas*

¿Qué medidas de seguridad utiliza en sus dispositivos móviles y computadoras? *Patrón*

¿Qué tanto conoce sobre estafas en línea (phishing) y programas maliciosos (malware)? *Desconoce*

II. Diseño de la Plataforma

¿Qué características considera importantes en una plataforma de aprendizaje en línea? *más fácil*

¿Cuáles serían las principales dificultades que enfrentaría para utilizar una plataforma de ciberseguridad? *internet.*

¿En qué dispositivos suele acceder a plataformas educativas en línea (computadora, celular, Tablet)? *celular.*

III. Desarrollo del Prototipo

¿Qué tan fácil o difícil le resulta navegar en plataformas digitales? *fácil*

¿Qué tipo de herramientas o funcionalidades le gustaría encontrar en la plataforma para facilitar su aprendizaje? *interactivo*

IV. Módulos Educativos

¿Qué aspectos específicos sobre phishing y malware le gustaría aprender? *todo sobre el tema*

¿Considera que los ejemplos prácticos y simulaciones ayudarían a su aprendizaje?

¿Por qué? *sería bueno aprender*

¿Qué tipo de actividades o materiales educativos (videos, lecturas, cuestionarios) prefiere? *cuestionarios*

Fuente: Elaboración propia

Figura 12: Resultados de la Entrevista

V. Manual de Usuario

¿Prefiere manuales escritos, tutoriales en video o sesiones interactivas para aprender a usar una nueva plataforma?

Secciones interactivas
 ¿Qué información le gustaría que incluyera un manual de usuario para la plataforma de aprendizaje? *seria mas informacion*

VI. Comentarios Finales

¿Qué otras sugerencias tienen para mejorar la enseñanza de ciberseguridad en su comunidad?

seria bueno aprender de la tecnologia y seguridad

Fuente: Elaboración propia

Figura 13: Resultados de la Entrevista

Universidad Central de Nicaragua
Campus Central
Facultad de Ingeniería en Sistemas
Entrevista dirigida a los Habitantes de la Comunidad Monte Fresco

Fecha: 08/02/2025 Hora inicio: 9:00 Pm Hora Final: 9:09 Pm
 Nombre del entrevistado: Bryan Sevilla

La presente entrevista tiene como objetivo recopilar información del tema de estudio: "Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, Managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025." para optar de Ingeniero en sistemas. Los datos proporcionados serán tratados con prudencia y serán totalmente confidenciales, dicha investigación ayudara a la investigación para indagar sobre el tema de estudio. De esta recopilación se presentarán los resultados, conclusiones y recomendaciones. De ante mano se agradece la disponibilidad y el apoyo brindado para esta investigación.

I. Identificación de Necesidades de Formación.

¿Ha escuchado hablar sobre las estafas digitales?
Si he escuchado

¿Sabe que el mal uso de dispositivos móviles o plataformas puede ocasionar el robo de información o dinero?

En su hogar, ¿usan celulares inteligentes, laptops o computadoras de escritorio?

¿En su comunidad han recibido capacitaciones sobre el uso seguro de la tecnología?
No

¿Ha participado en cursos o talleres sobre cómo proteger su información digital?
No

¿Le gustaría recibir asesoría o capacitación sobre el uso seguro de dispositivos móviles y computadoras?
Si

Fuente: Elaboración propia

Figura 14: Resultados de la Entrevista

¿Qué temas considera importantes para proteger su información digital en sus dispositivos? *Uso de Contraseña*

¿Qué medidas de seguridad utiliza en sus dispositivos móviles y computadoras?

¿Qué tanto conoce sobre estafas en línea (phishing) y programas maliciosos (malware)? *Desconoce.*

II. Diseño de la Plataforma

¿Qué características considera importantes en una plataforma de aprendizaje en línea? *Desarrollo*

¿Cuáles serían las principales dificultades que enfrentaría para utilizar una plataforma de ciberseguridad? *Ninguna.*

¿En qué dispositivos suele acceder a plataformas educativas en línea (computadora, celular, Tablet)? *Celulares.*

III. Desarrollo del Prototipo

¿Qué tan fácil o difícil le resulta navegar en plataformas digitales?

Fácil
¿Qué tipo de herramientas o funcionalidades le gustaría encontrar en la plataforma para facilitar su aprendizaje?

IV. Módulos Educativos

¿Qué aspectos específicos sobre phishing y malware le gustaría aprender?

Todo sobre ellos.
¿Considera que los ejemplos prácticos y simulaciones ayudarían a su aprendizaje?

¿Por qué? *Si lo considero que si*

¿Qué tipo de actividades o materiales educativos (videos, lecturas, cuestionarios) prefiere? *1*

Fuente: Elaboración propia

Figura 15: Resultados de la Entrevista**V. Manual de Usuario**

¿Prefiere manuales escritos, tutoriales en video o sesiones interactivas para aprender a usar una nueva plataforma? *Sesiones interactivas*

¿Qué información le gustaría que incluyera un manual de usuario para la plataforma de aprendizaje? *Respaldo de datos.*

VI. Comentarios Finales

¿Qué otras sugerencias tienen para mejorar la enseñanza de ciberseguridad en su comunidad? *Cursos Para Ciberseguridad.*

Fuente: Elaboración propia

Figura 16: Resultados de la Entrevista

Universidad Central de Nicaragua
Campus Central
Facultad de Ingeniería en Sistemas
Entrevista dirigida a los Habitantes de la Comunidad Monte Fresco

Fecha: 08/Feb/2025 Hora inicio: 9:30 pm HoraFinal: 9:37 pm.
 Nombre del entrevistado: Jean Carlos Pastran Gaitan.

La presente entrevista tiene como objetivo recopilar información del tema de estudio: "Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, Managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025." para optar de Ingeniero en sistemas. Los datos proporcionados serán tratados con prudencia y serán totalmente confidenciales, dicha investigación ayudara a la investigación para indagar sobre el tema de estudio. De esta recopilación se presentarán los resultados, conclusiones y recomendaciones. De ante mano se agradece la disponibilidad y el apoyo brindado para esta investigación.

I. Identificación de Necesidades de Formación.

¿Ha escuchado hablar sobre las estafas digitales?

Sí

¿Sabe que el mal uso de dispositivos móviles o plataformas puede ocasionar el robo de información o dinero?

Sí

En su hogar, ¿usan celulares inteligentes, laptops o computadoras de escritorio?

Celulares y laptops.

¿En su comunidad han recibido capacitaciones sobre el uso seguro de la tecnología? NO.

¿Ha participado en cursos o talleres sobre cómo proteger su información digital?

NO.

¿Le gustaría recibir asesoría o capacitación sobre el uso seguro de dispositivos móviles y computadoras?

Sí

Fuente: Elaboración propia

Figura 17: Resultados de la Entrevista

¿Qué temas considera importantes para proteger su información digital en sus dispositivos? *Contraseñas.*

¿Qué medidas de seguridad utiliza en sus dispositivos móviles y computadoras?

Contraseñas.

¿Qué tanto conoce sobre estafas en línea (phishing) y programas maliciosos (malware)? *Desconozco*

II. Diseño de la Plataforma

¿Qué características considera importantes en una plataforma de aprendizaje en línea? *Fácil uso.*

¿Cuáles serían las principales dificultades que enfrentaría para utilizar una plataforma de ciberseguridad? *No tener conocimiento*

¿En qué dispositivos suele acceder a plataformas educativas en línea (computadora, celular, Tablet)?

Celular.

III. Desarrollo del Prototipo

¿Qué tan fácil o difícil le resulta navegar en plataformas digitales?

Fácil.
¿Qué tipo de herramientas o funcionalidades le gustaría encontrar en la plataforma para facilitar su aprendizaje?

Manual

IV. Módulos Educativos

¿Qué aspectos específicos sobre phishing y malware le gustaría aprender?

Todo

¿Considera que los ejemplos prácticos y simulaciones ayudarían a su aprendizaje?

¿Por qué? *Sí, ayuda al uso.*

¿Qué tipo de actividades o materiales educativos (videos, lecturas, cuestionarios) prefiere?

Todo

Fuente: Elaboración propia

Figura 18: Resultados de la Entrevista

V. Manual de Usuario

¿Prefiere manuales escritos, tutoriales en video o sesiones interactivas para aprender a usar una nueva plataforma?

tutoriales en video
¿Qué información le gustaría que incluyera un manual de usuario para la plataforma de aprendizaje?

Responde de datos.

VI. Comentarios Finales

¿Qué otras sugerencias tienen para mejorar la enseñanza de ciberseguridad en su comunidad?

Cursos de ciberseguridad.

Fuente: Elaboración propia

Figura 19: Resultados de la Entrevista

Universidad Central de Nicaragua
Campus Central
Facultad de Ingeniería en Sistemas

Entrevista a un Representante del CPC en Monte Fresco

Fecha: 15/02/2025 Hora inicio: 4:00 Pm Hora Final: 4:20 Pm
Nombre del entrevistado: Alba Mercedes Mubien Forero

La presente entrevista tiene como objetivo recopilar información del tema de estudio: "Desarrollo de un prototipo de una plataforma de aprendizaje en la ciberseguridad dirigido a la comunidad de Monte Fresco del municipio de villa el Carmen, Managua Nicaragua, en el periodo de Mes de noviembre del 2024 a febrero del año 2025." para optar de Ingeniero en sistemas. Los datos proporcionados serán tratados con prudencia y serán totalmente confidenciales, dicha investigación ayudara a la investigación para indagar sobre el tema de estudio. De esta recopilación se presentarán los resultados, conclusiones y recomendaciones. De ante mano se agradece la disponibilidad y el apoyo brindado para esta investigación.

1. Sobre la comunidad y el uso de la tecnología

- ¿Qué porcentaje de los habitantes de Monte Fresco utiliza dispositivos tecnológicos? 90% de los habitantes
- ¿Cuáles son los principales dispositivos tecnológicos que usan los habitantes de Monte Fresco en su vida diaria? (Ejemplo: celulares, computadoras, tabletas) la mayoría de personas celulares
- ¿Qué tan informados están los habitantes de Monte Fresco sobre estafas digitales y amenazas en la red? Muy poco informados
- ¿Qué plataformas o redes sociales son más utilizadas en la comunidad? facebook, whatsapp, tiktok
- ¿Existen grupos de la comunidad que enfrentan más dificultades para el uso de la tecnología? (Ejemplo: adultos mayores, jóvenes, personas con poca educación formal) si Adultos mayores de 55 años
- ¿Qué tan accesible es el internet en la comunidad? ¿Las familias tienen conexión en sus hogares o dependen de puntos públicos de acceso? Es accesible en ciertos puntos de la comunidad
- ¿Existen programas o iniciativas en la comunidad para mejorar el acceso y el uso de la tecnología?
No

Fuente: Elaboración propia

Figura 20: Resultados de la Entrevista

2. Problemas y riesgos en el uso de la tecnología

1. ¿Se han reportado casos de fraudes en línea, robos de identidad u otros problemas de seguridad digital en la comunidad? *No se han repor*
2. ¿Considera que los habitantes de la comunidad suelen compartir información personal en redes sociales sin conocer los riesgos? *No, hay m
precaucion*
3. ¿Cuáles son los principales problemas que han enfrentado jóvenes y niños en el uso de la tecnología? (Ejemplo: acceso a contenido inapropiado, ciberacoso, adicción a pantallas) *el mayor problema es
adicción a pantallas*

3. Capacitaciones y conocimientos en ciberseguridad

1. ¿Alguna institución ha ofrecido capacitación sobre el uso seguro de la tecnología en la comunidad? Si es así, ¿qué temas han abordado? *si por parte del mate minet*
2. ¿Cree que los habitantes de la comunidad tienen conocimientos básicos sobre seguridad digital? ¿Sabían identificar estafas en línea como phishing o amenazas como malware? *si hay conocimiento pero poco*
3. ¿Qué tan interesada cree que estaría la comunidad en participar en talleres o capacitaciones sobre ciberseguridad? *habría interés
por parte de la comunidad*

4. Participación del CPC en el proyecto

1. ¿De qué manera cree que el CPC podría apoyar la implementación de un proyecto de capacitación en ciberseguridad en la comunidad?
2. ¿Existen espacios comunitarios adecuados para impartir talleres o sesiones de aprendizaje sobre ciberseguridad? (Ejemplo: centros comunitarios, escuelas, bibliotecas)
3. ¿Qué estrategias cree que serían más efectivas para motivar a más personas a participar en estas capacitaciones?

#1
Brindar apoyo mediante el uso de los
redes para darle publicidad al prototipo

#2
si, centros de estudio

#3
Demostrar la importancia de protegerse el
entorno digital

Fuente: Elaboración propia