UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Propuesta de programa de concienciación en ciberseguridad para usuarios de banca electrónica en la ciudad de Guayaquil

AUTOR
Mise Chica, Miguel Angel

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR
Cruz Carrillo, Henry Omar

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Cruz Carrillo, Ph.D.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR OVIEDO BAYAS

Ing. Byron Oviedo Bayas, Ph.D.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DIEGO EDUARDO BENAVIDES ASTUDILLO

Ing. Diego Benavides Astudillo, Ph.D.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **MISE CHICA MIGUEL ANGEL**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Omar Cruz Carrillo, PhD.

Santa Elena, 30 de junio 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **MISE CHICA MIGUEL ANGEL**

DECLARO QUE:

El trabajo de Titulación, **PROPUESTA DE PROGRAMA DE CONCIENCIACIÓN EN CIBERSEGURIDAD PARA USUARIOS DE BANCA ELECTRÓNICA EN LA CIUDAD DE GUAYAQUIL,** previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 30 de junio 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MIGUEL ANGEL MISE CHICA

Mise Chica Miguel Angel

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **PROPUESTA DE PROGRAMA DE CONCIENCIACIÓN EN CIBERSEGURIDAD PARA USUARIOS DE BANCA ELECTRÓNICA EN LA CIUDAD DE GUAYAQUIL**, presentado por el estudiante, **MISE CHICA MIGUEL ANGEL** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Certificado de análisis
Compilatio Magister+ | ESPE-ECU

Miguel Mise - Componente Practico - analisis
ID : b60427e93125f7067ab6bc1c71f111fcba7bdfa0

6%
Textos sospechosos

Nombre del fichero : Miguel Mise - Componente Practico - analisis.txt
Tamaño del archivo original : 4,19 MB
Número de palabras : 7725

Depositante : HENRY OMAR CRUZ CARRILLO
Fecha de depósito : 1 de julio de 2026
Tipo de carga : interface
fecha de fin de análisis : 1 de julio de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Omar Cruz Carrillo, PhD.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **MISE CHICA MIGUEL ANGEL**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 30 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MIGUEL ANGEL MISE CHICA

Mise Chica Miguel Angel

AGRADECIMIENTO

Deseo expresar mi más profundo y sincero agradecimiento a mi familia, por ser el pilar fundamental en mi vida y la fuente de motivación inagotable que me permitió perseverar en los momentos de mayor exigencia académica. Este logro es, en gran medida, fruto del apoyo constante que me brindaron en cada etapa de este camino. También extiendo mi gratitud a la empresa que permitió aplicar los conocimientos adquiridos en un entorno real, fortaleciendo así mi compromiso con la excelencia y la seguridad de la información.

Miguel Angel, Mise Chica

DEDICATORIA

Dedicó este trabajo a aquellos valientes que, enfrentando diversas adversidades, tuvieron que interrumpir sus estudios por alguna razón, pero encontraron la fuerza para retomarlos. Su constancia e insistencia en buscar el conocimiento constituyen una fuente de inspiración. Que este documento actúe como recordatorio de que las dificultades se pueden superar y que el aprendizaje representa un viaje eterno que nunca debe ser abandona.

Miguel Angel, Mise Chica

ÍNDICE GENERAL

TRIBUNAL DE SUSTENTACIÓN II
CERTIFICACIÓN III
DECLARACIÓN DE RESPONSABILIDAD IV
CERTIFICACIÓN DE ANTIPLAGIO V
AUTORIZACIÓN VI
AGRADECIMIENTO VII
DEDICATORIA VIII
ÍNDICE GENERAL IX
ÍNDICE DE TABLAS XIII
ÍNDICE DE FIGURAS XIV
RESUMEN XV
ABSTRACT XVI
INTRODUCCIÓN 1
CAPÍTULO 1 4
1. FUNDAMENTACIÓN 4
1.1.1 ANTECEDENTES 4
1.1.2 DESCRIPCIÓN DEL PROYECTO 5
1.2 OBJETIVOS DEL PROYECTO 6
1.2.1 OBJETIVO GENERAL 6

1.2.2 OBJETIVOS ESPECÍFICOS 6
1.3 JUSTIFICACIÓN DEL PROYECTO 7
1.4 ALCANCE DEL PROYECTO 8
CAPÍTULO 2 10
2.1 ESTABLECIMIENTO DE LA LÍNEA BASE 10
2.1.1 Técnicas e Instrumentos Utilizados 10
2.1.2 Resultados de la Línea Base (Simulación Gophish) 11
2.1.3 Evaluación mediante Matriz de Riesgo 12
2.1.4 Matriz de Hallazgos en la Línea Base 12
CAPÍTULO 3 14
3.1 MARCO TEÓRICO 14
3.1.1 La Ciberseguridad y el Factor Humano 14
3.1.2 Ingeniería Social 15
3.1.3 El Modelo KAB 16
3.1.4 Estándares Internacionales y Normativa Legal 17
3.1.5 Propuestas Existentes en Ciberseguridad 18
3.2 METODOLOGÍA DE INVESTIGACIÓN 19
3.2.1 Métodos Aplicados 19
3.2.2 Procesamiento de Datos 20
3.3 TECNICAS DE RECOLECCIÓN DE INFORMACIÓN 21
3.3.1 Simulación Automatizada de Ingeniería Social 21
3.4 POBLACIÓN Y MUESTRA 22

3.4.1 Consideraciones Éticas y Consentimiento 23
CAPÍTULO 4 24
4.1 PROPUESTA 24
4.1.1 Materiales del Programa 24
4.1.2 Desarrollo de la Propuesta Educativa 25
RESULTADOS 28
5.1 Análisis de los Resultados y Cambio Conductual 30
5.2 Análisis Estadístico Inferencial y Prueba de Hipótesis 31
5.3 Selección de la Prueba y Nivel de Significancia 31
5.4 Análisis Estadístico 34
CONCLUSIONES 35
RECOMENDACIONES 37
REFERENCIAS 39
ANEXOS 42
Anexo 1: Telemetría de la Campaña de Simulación de Phishing (Línea Base - Pre-test) 42
Anexo 2: Diseño de la Plantilla de Phishing Simulado - Escenario de Urgencia 43
Anexo 3: Diseño de la Página de Captura de Credenciales 44
Anexo 4: Carta de Autorización Institucional y Consentimiento de Participación. 45
Anexo 5: Interfaz Principal y Tablero de Control 46
Anexo 6: Cápsulas de Aprendizaje Interactivo (Modelo KAB) 47
Pantalla Módulo 1 47
Pantalla Módulo 2 48

Pantalla Módulo 3 49
Anexo 7: Sistema de Evaluación en el Cliente y Certificación Automática..... 50
Pantalla de preguntas de evaluación del módulo 50
Pantalla de resultados de evaluación..... 50
Pantalla de presentación de diploma de completar el curso. 51
Anexo 8: Telemetría de Resultados - Campaña Post-test (Gophish)..... 52
Resultados de la Campaña 52
Detalle Granular de Interacción por Usuario 52
Anexo 9: Diseño de la Plantilla de Phishing Simulado (Post-test) - Escenario Administrativo53
Anexo 10: Diseño de la Página de Captura de Credenciales (Post-test) - Clonación de CRM 54

ÍNDICE DE TABLAS

Tabla 1- Perfil de Vulnerabilidad KAB (Simulación Pre-test) 12

Tabla 2- Matriz de Brechas Críticas (Pre-test) 13

Tabla 3- Ataques de Ingeniería Social 15

Tabla 4- Niveles Modelo KAB 17

Tabla 5 - Estructura Comparativa y Pedagógica de los Módulos 27

Tabla 6 - Comparativa de Vulnerabilidad KAB (Pre-test vs. Post-test) 29

Tabla 7- Tabla de Contingencia (Distribución de Frecuencias Pareadas) 32

Tabla 8 - Resultados de la Prueba de Hipótesis y Tamaño del Efecto 33

ÍNDICE DE FIGURAS

Figura 1- Incidentes de extorsión de datos y ransomware en 2024 1

Figura 2- Tablero de control sistema Gophish..... 42

Figura 3- Plantilla correo campaña inicial 43

Figura 4 - Diseño página web de captura de credenciales 44

Figura 5 - Carta de autorización..... 45

Figura 6 - Interfaz principal programa capacitación..... 46

Figura 7- Módulo 1 programa capacitación..... 47

Figura 8 - Módulo 2 programa capacitación..... 48

Figura 9 - Módulo 3 programa capacitación..... 49

Figura 10 - Interfaz de preguntas programa capacitación..... 50

Figura 11 - interfaz de vista de resultados programa capacitación 50

Figura 12 - Certificación de completar el programa de capacitación 51

Figura 13 - Resultados de campaña Post Test 52

Figura 14 - Evidencia de captura de credenciales..... 52

Figura 15 - Diseño plantilla Post Test..... 53

Figura 16 - Diseño página web captura de credenciales Post Test 54

RESUMEN

El presente trabajo se enfoca en la debilidad de las personas frente a la amenaza de ingeniería social relacionada con el ámbito bancario en la ciudad de Guayaquil. El propósito central ha sido concebir un plan de formación en ciberseguridad, apoyado en el modelo KAB (Conocimiento, Actitud y Comportamiento).

La metodología empleada consistió en una investigación de enfoque cuantitativo con un alcance descriptivo-propositivo, utilizando como caso de estudio a una muestra de 30 colaboradores de una empresa privada de la ciudad de Guayaquil. El análisis inicial, reveló un estado de vulnerabilidad en un nivel severo, lo que indica un comportamiento de los individuos de prueba en un nivel de riesgo crítico.

Luego de la ejecución de un piloto del programa de concienciación, los análisis de los resultados de la simulación reflejaron una disminución representativa en la tasa de interacción con amenazas, logrando bajar el estado de vulnerabilidad a un nivel de riesgo bajo. Se concluye que el programa diseñado, apoyado en métricas objetivas de software, constituye una herramienta eficaz para mitigar el riesgo humano de ser víctima de estafas con ingeniería social, transformando al usuario de un eslabón débil a un sensor activo de amenazas en el ecosistema digital de Guayaquil.

Palabras clave: Ciberseguridad, Ingeniería Social, Modelo KAB, Phishing Simulado.

ABSTRACT

This study focuses on the vulnerability of individuals to the threat of social engineering within the banking sector in the city of Guayaquil. Its central purpose has been to devise a cybersecurity training plan, based on the KAB model (Knowledge, Attitude, and Behavior).

The methodology employed followed a quantitative approach with a descriptive-propositional scope, using as a case study a sample of 30 employees from a private company in the city of Guayaquil. The initial analysis revealed a severe level of vulnerability, indicating that the behavior of the participants corresponded to a critical risk level.

After the implementation of a pilot version of the awareness program, the analysis of simulation results showed a significant decrease in the rate of interaction with threats, reducing the vulnerability status to a low-risk level. It is concluded that the designed program, supported by objective software-based metrics, constitutes an effective tool to mitigate the human risk of falling victim to social engineering scams, transforming the user from a weak link into an active threat sensor within the digital ecosystem of Guayaquil.

Keywords: Cybersecurity, Social Engineering, KAB Model, Simulated Phishing.

INTRODUCCIÓN

En los tiempos que corren, el acceso a la tecnología ha cambiado la manera en que los ciudadanos interactúan con el sistema financiero en Ecuador. Según el LATAM Regional Threat Landscape Report elaborado por CrowdStrike (2025), En América Latina se experimentó una creciente ola de campañas de ataques con ingeniería social, impulsadas tanto por actores locales como internacionales.

Como se observa en la Figura 1, durante el 2024 los ataques de extorsión de datos conocido como ransomware afectaron especialmente a sectores como tecnología, servicios financieros, servicios de salud y el comercio minorista, evidenciando una evolución constante en las tácticas utilizadas por los atacantes.

Figura 1- Incidentes de extorsión de datos y ransomware en 2024

Esto tiene especial relevancia para ciudades altamente digitalizadas como Guayaquil, donde la adopción de la banca electrónica ha crecido de manera sostenida en los últimos años, destacando que los servicios financieros se encuentran entre los sectores más afectados por extorsión digital y ataques con ingeniería social en la región.

Esta tendencia deja en evidencia que, incluso con avances en infraestructura tecnológica, si hay falta de capacitación en ciberseguridad para los usuarios este se convierte en un punto crítico.

En este contexto, un programa de concienciación dirigido a los usuarios de banca electrónica se convierte en una medida clave para reducir vulnerabilidades y fortalecer la resiliencia digital del usuario ciudadano de Guayaquil.

En este trabajo se abordó la necesidad de fortalecer la cultura de ciberseguridad entre los usuarios de banca electrónica en la ciudad de Guayaquil, tomando como caso de estudio el análisis del entorno operativo de la empresa Heurística S.A. en la ciudad de Guayaquil, cuya sucursal local maneja información altamente sensible y refleja de manera representativa los riesgos a los que se enfrenta cualquier ciudadano al interactuar digitalmente con servicios financieros.

La variedad de perfiles y el manejo constante de datos personales y bancarios permiten comprender cómo los ataques de ingeniería social se apoyan principalmente en fallas humanas más que tecnológicas.

A partir de este contexto, la investigación plantea como objetivo diseñar un programa de concienciación en ciberseguridad fundamentado en el modelo que integra conocimiento, actitud y comportamiento (KAB). Para lo cual se implementó una evaluación basada en telemetría de interacciones reales mediante simulaciones automatizadas de *phishing*, estandarizadas a través de una Matriz de Riesgo.

Aunque este caso de estudio se desarrolla en una sola empresa, la propuesta aspira a ser un modelo replicable en toda la ciudad de Guayaquil, aportando valor social al proteger la

información de los ciudadanos y contribuyendo al desarrollo de un marco metodológico medible, objetivo y escalable para fortalecer la ciberseguridad en el contexto ecuatoriano.

CAPÍTULO 1

1. FUNDAMENTACIÓN

1.1.1 ANTECEDENTES

En todo el mundo, la ciberseguridad pasó de ser un asunto exclusivamente técnico a un componente crítico de estabilidad, con campañas que explotan las vulnerabilidades del factor humano como phishing, entre otras, de hecho, tres de cada cuatro responsables de seguridad de la información han identificado el error humano como el principal riesgo de ciberseguridad (Proofpoint, 2024). En Ecuador, el uso de canales digitales se aceleró de gran manera: en 2023 se realizaron 228 millones de transferencias interbancarias por USD 191.205 millones, y el número de operaciones con medios electrónicos se triplicó respecto de 2019 (BCE, 2024). En paralelo, América Latina tiene registros de 1.291 millones de intentos de phishing bloqueados en 12 meses, impulsados por campañas automatizadas con Inteligencia Artificial y smishing masivo, lo que incrementa la exposición del usuario común de banca electrónica (Kaspersky, 2025).

En este marco, la sucursal Guayaquil de Heurística S.A. que gestiona información sensible en procesos de cobranza, resulta un escenario representativo para observar cómo gran parte de los ataques digitales exitosos no vulneran el software, sino la confianza del usuario a través de tácticas como el phishing entre otras. Por lo tanto, Heurística S.A. constituye un caso de estudio idóneo para implementar un programa de concienciación que sea medible y escalable al contexto de Guayaquil.

1.1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto consiste en el diseño de un programa integral de concienciación en ciberseguridad, estructurado bajo el modelo KAB (Knowledge, Attitude, Behavior), orientado a mitigar los riesgos de ingeniería social en los usuarios de banca electrónica de la ciudad de Guayaquil, utilizando a la empresa Heurística S.A. como el entorno de validación y caso de estudio piloto.

Al ser un trabajo de carácter práctico-propositivo, el alcance se centra en la estructuración técnica del programa y una validación de efectividad con un piloto, cuya ejecución metodológica se divide en tres fases fundamentales:

- **Fase de Diagnóstico y Línea Base**: Despliegue de simulaciones ofensivas controladas para identificar, mediante telemetría real, las vulnerabilidades del personal frente a tácticas de ingeniería social.
- **Fase de Diseño Curricular:** Desarrollo de la propuesta educativa bajo un formato de Microlearning asincrónico. Se estructura el contenido pedagógico en módulos interactivos diseñados para el usuario final, traduciendo el lenguaje técnico a un formato comprensible y accesible.
- **Fase de Framework de Evaluación:** Establecimiento de un sistema de métricas cuantitativas basado en simulaciones automatizadas de phishing y analizado mediante una Matriz de Riesgo de 4 niveles.

En cuanto a las tecnologías y herramientas utilizadas en el proyecto detalla la siguiente arquitectura:

- El uso de la plataforma de simulación de ataques Gophish (Gophish, 2024) que es Open Source como instrumento de auditoría y medición.
- El diseño de un prototipo interactivo web (HTML/JS) libre de dependencias, como la interfaz visual para la entrega del material pedagógico.

1.2 OBJETIVOS DEL PROYECTO

1.2.1 OBJETIVO GENERAL

Diseñar una propuesta de programa de concienciación en ciberseguridad para usuarios de banca electrónica en la ciudad de Guayaquil, mediante el estudio de caso en la empresa Heurística S.A., orientado a reducir la vulnerabilidad frente a ataques de ingeniería social.

1.2.2 OBJETIVOS ESPECÍFICOS

1. Establecer la línea base diagnóstica en la sucursal de Guayaquil de la empresa Heurística S.A. mediante simulaciones controladas de ingeniería social, para identificar las brechas conductuales del personal.

2. Analizar las propuestas existentes en el estado del arte y marcos de referencia internacionales relacionados con la concienciación en ciberseguridad para fundamentar metodológicamente la estructura del programa.

3. Diseñar la estructura del programa de concienciación en formato de Microlearning asincrónico, orientado a mitigar los riesgos de fraude en servicios financieros digitales.

4. Medir el impacto del programa de capacitación implementando un grupo piloto respaldando los hallazgos con un análisis estadístico.

1.3 JUSTIFICACIÓN DEL PROYECTO

Realizar este trabajo fue necesario porque la debilidad más grande en la cadena de seguridad de los usuarios de servicios financieros digitales no reside en la tecnología de infraestructura, sino en los usuarios mismos.

Según datos del Banco Central del Ecuador en 2024, el uso de medios electrónicos fue el triple con respecto a 2019, alcanzando transacciones por USD 191.205 millones solo en 2023 y este aumento ha convertido a cualquier ciudadano que utiliza un teléfono inteligente o acceso a internet en un objetivo lucrativo para ser víctima de campañas de ingeniería social (Kaspersky, 2025).

En Guayaquil, que concentra el 45% de los usuarios de banca electrónica del país, la exposición al fraude digital es cada vez mayor. La elección de Heurística S.A. como caso de estudio no responde a su giro de negocio, sino a que su personal constituye una muestra representativa de la diversidad de usuarios de banca en la ciudad.

El ambiente con personas con niveles educativos diferentes que usan aplicaciones móviles y reciben comunicaciones electrónicas diariamente. Teniendo el acceso controlado y el

consentimiento informado de este grupo permiten validar la efectividad de un programa de concienciación antes de ser escalado a la población general.

Lo que se busca con este programa es enseñar a las personas a detectar amenazas reales en sus vidas cotidianas. Se pretende que el usuario adquiera la habilidad de identificar fraudes comunes, tales como un mensaje engañoso para actualización de datos personales o un supuesto correo del banco que oculta un archivo malicioso. Desde el punto de vista social, la herramienta reconoce una manera de prevenir el daño financiero e informático en Guayaquil, además está alineada con la Ley Orgánica de Protección de Datos Personales (LOPDP).

En cuanto a su relevancia científica, destacamos la incorporación de herramientas como Gophish para evaluar la educación del personal. En lugar de limitarse a una capacitación convencional, proponemos una auditoría técnica medible. Este marco de trabajo queda abierto para que cualquier organización lo implemente y mida el nivel de riesgo real de su factor humano.

1.4 ALCANCE DEL PROYECTO

Este trabajo se estructura como una propuesta técnica y metodológica. Su alcance abarca la creación de la propuesta de un programa de concienciación en ciberseguridad, diseñado para ser accesible a cualquier usuario final.

La delimitación detalla en los siguientes puntos:

1. **Delimitación de Población:** Para la validación del diseño, se utilizará como grupo piloto representativo al personal de la empresa de Heurística S.A. (Sucursal Guayaquil), quienes

participarán bajo consentimiento informado como una muestra de usuarios de servicios financieros digitales en la urbe.

2. **Delimitación Funcional:**

   Evaluación objetiva del nivel de conocimientos, actitudes e intervenciones del grupo objeto de estudio hacia riesgos diarios, realizado mediante simulaciones de ingeniería social controladas, desarrollo de módulos formativos en formato de microlearning interactiva **y** construcción de un Matriz de Riesgo basado en datos telemétricos de las pruebas.

3. **Delimitación Técnica:** El programa se enfoca exclusivamente en análisis de resultados de simulaciones y prevención de ataques de ingeniería social. No incluye desarrollos de software de seguridad ni auditorías de infraestructuras de red ni configuraciones de sistemas bancarios.
4. **Exclusiones**: El trabajo consiste exclusivamente en ejecutar una prueba piloto con el grupo objetivo para probar la viabilidad del diseño sugerido en términos estadísticos.

CAPÍTULO 2

2.1 ESTABLECIMIENTO DE LA LÍNEA BASE

El establecimiento de la línea base permite determinar el estado actual de los usuarios frente a las amenazas de ingeniería social antes de cualquier intervención. Este diagnóstico se convierte en el punto de comparación cuantitativo para medir la efectividad de la propuesta de concienciación; este diagnóstico inicial tiene como propósito caracterizar el nivel de vulnerabilidad del grupo piloto frente a las amenazas de ingeniería social. Sin este diagnóstico previo, cualquier afirmación sobre el impacto del programa carecería de sustento empírico y comparativo.

2.1.1 Técnicas e Instrumentos Utilizados

Para el levantamiento de esta línea base en el grupo piloto se empleó de manera objetiva y coordinada la herramienta de Simulación Automatizada de Ingeniería Social Gophish, la cual constituye el instrumento principal y de grado profesional.

Mediante el despliegue de un escenario ciego de *phishing* controlado, se evaluaron las tres dimensiones del modelo KAB a través de las interacciones reales del usuario con el sistema, sin que este supiera que estaba siendo evaluado.

Es importante aclarar que la **Tasa de Apertura** funciona únicamente como una métrica de alcance y exposición, es decir medir que la simulación llego a todos los objetivos seleccionados, validando que el correo superó los filtros *antispam* y que el usuario cumplió su rutina laboral de revisión.

El nivel de vulnerabilidad real esta mapeado en las siguientes dimensiones:

- ***Conocimiento (K) - Tasa de Clics:*** Evalúa si el usuario hace clic tras abrir el correo, analizando su conocimiento básico para identificar las señales de phishing.
- ***Actitud (A) - Captura de Credenciales:*** Mide la disposición a confiar ciegamente. Evalúa cuántos usuarios ignoraron el riesgo de la página clonada e ingresaron sus datos.
- ***Comportamiento (B) - Reportar:*** Registra la acción de mitigación segura. Evalúa si el usuario ejecutó el protocolo correcto alertando al área técnica.

2.1.2 Resultados de la Línea Base (Simulación Gophish)

Para establecer el nivel de vulnerabilidad real del grupo piloto, se ejecutó una campaña ciega de *phishing* simulado (ver evidencia en el Anexo 1). La campaña fue enviada a los 30 colaboradores de la muestra bajo un escenario de suplantación de identidad (ver diseño del correo y página falsa en los Anexos 2 y 3) con pretexto de urgencia sobre la caducidad de contraseñas.

Los resultados extraídos directamente del dashboard de la plataforma arrojaron las siguientes métricas de interacción:

- **Correos enviados:** 30
- **Correos abiertos (*Tasa de Apertura*):** 30 (100.00%)
- **Clics en enlaces maliciosos (Tasa de *Clic*):** 19 (63.33%)
- **Datos/Credenciales ingresadas (*Tasa Captura Credenciales*):** 8 (26.67%)
- **Correos reportados a TI (Tasa de Reporte):** 1 (3.33%)

2.1.3 Evaluación mediante Matriz de Riesgo

Para transformar los porcentajes operativos arrojados por el software en indicadores comprensibles de auditoría, se adoptó una **Matriz de Riesgo de 4 Niveles**. Esta metodología estandarizada asigna el nivel de vulnerabilidad de forma directa según el porcentaje de fallo del usuario (donde un mayor porcentaje de interacción con la amenaza o falta de acción preventiva indica mayor riesgo):

- **Nivel 1 (Riesgo Bajo):** De 0% a 25% de fallos.
- **Nivel 2 (Riesgo Medio):** De 26% a 50% de fallos.
- **Nivel 3 (Riesgo Alto):** De 51% a 75% de fallos.
- **Nivel 4 (Riesgo Crítico):** De 76% a 100% de fallos.

Aplicando este estándar directo a los resultados obtenidos, se establece el perfil de vulnerabilidad inicial de la organización los resultados se muestran en la Tabla 1:

Tabla 1- Perfil de Vulnerabilidad KAB (Simulación Pre-test)

Dimensión	Métrica de Evaluación	Tasa de Fallo (%)	Nivel de Riesgo
Conocimiento	Tasa de Clics	63.33	Alto
Actitud	Tasa de Captura de Credenciales	26.67	Medio
Comportamiento	No Reportada incidente	96.67	Crítico

2.1.4 Matriz de Hallazgos en la Línea Base

El análisis de los datos extraídos de la plataforma permite identificar tres brechas críticas de seguridad que fundamentan la necesidad del programa de concienciación, se puede ver los valores de la matriz de brechas en la Tabla 2:

Tabla 2- Matriz de Brechas Críticas (Pre-test)

Brecha Identificada en el Sistema	**Dimensión afectada**	**Evidencia del Software**	**Nivel de Riesgo**
Falta de discernimiento visual	Conocimiento	El 63.33% de la muestra no identificó las señales de alerta de *phishing* y procedió a hacer clic en el enlace malicioso.	Alto
Confianza ciega para entregar datos	Actitud	El 26.67% de la muestra ignoró el riesgo de la página de destino fraudulenta e ingresó sus credenciales.	Medio
Ausencia de protocolo de reporte	Comportamiento	El 96.67% de la muestra no utilizó los canales correspondientes para reportar el correo sospechoso al área de TI.	Crítico

Entre los hallazgos más preocupantes está la falta significativa de conocimiento respecto al reconocimiento visual de amenazas. Aunque la mayor parte de las respuestas abrieron y visualizaron el correo electrónico, casi la totalidad del personal (63.33%) no identificó el engaño y accedió a el enlace malicioso. También destaca la inacción constante dado que la mayoría de la gente no realizo ningún proceso de denuncia, esto demuestra que el personal no actúa como un sistema activo de detección de riesgos.

Estos resultados evidencian que la manipulación con ingeniería social es altamente efectiva en este grupo, validando la urgencia de implementar el programa de concienciación propuesto.

CAPÍTULO 3

3.1 MARCO TEÓRICO

3.1.1 La Ciberseguridad y el Factor Humano

La ciberseguridad ha evolucionado de un enfoque puramente perimetral y técnico hacia uno centrado en las personas. Durante mucho tiempo, las empresas han invertido principalmente en soluciones tecnológicas como firewalls, sistemas de detección de intrusos y el cifrado de los datos que manejan; sin embargo, todas estas medidas no son suficientes frente a ataques que explotan errores y decisiones de los usuarios lo que pone en claro una realidad contundente: el eslabón más débil sigue siendo el usuario es decir el componente humano el cual suele ser un punto de entrada altamente explotado por los atacantes.

El Data Breach Investigations Report (Verizon, 2024) muestra que más de dos tercios de las brechas aproximadamente el 68% involucran un componente humano, lo que confirma que los atacantes siguen prefiriendo vectores que manipulan conductas antes que vulnerabilidades puramente técnicas.

Esta información refleja que las vulnerabilidades no residen únicamente en los sistemas y aplicaciones que utilizamos a diario, sino en los comportamientos, hábitos y las decisiones de quienes operan estos sistemas. Por esto expuesto la concienciación en seguridad informática ha dejado de ser un complemento opcional para convertirse en una barrera de defensa para lograr modificar actitudes y reducir el comportamiento de riesgo de los usuarios. Por tanto, comprender el rol del factor humano no solo permite identificar las causas raíz de muchos incidentes, sino también diseñar estrategias preventivas más efectivas que complementen las soluciones técnicas existentes.

3.1.2 Ingeniería Social

La ingeniería social en el ámbito de este proyecto se define como el conjunto de técnicas orientadas a engañar a las personas para que revelen información sensible o ejecuten acciones que comprometan la seguridad, en la Tabla 3 se detalla los ataques más conocidos.

Tabla 3- Ataques de Ingeniería Social

Ataque	**¿Qué busca el atacante?**	**Vectores/medios habituales**
Phishing	Captura de credenciales o ejecución de acciones no deseadas.	Correos o mensajes con enlaces que redirigen a páginas peligrosas o inician descargas.
Robo de datos	Acceso directo a cuentas y sistemas con usuario y contraseña robadas.	Mensajes con phishing, y en portales o aplicaciones que simulan ser sitios lícitos.
Suplantación de identidad	Obtener claves, guiar al usuario a enlaces maliciosos	Llamadas telefónicas y mensajes
Ransomware	Cifrado y/o exfiltración de datos con fines de extorsión.	Campañas que comienzan en correo/servicios y terminan en ransomware/extorsión

3.1.3 El Modelo KAB

Históricamente, el modelo KAB (por sus siglas en inglés: *Knowledge, Attitudes, and Behavior*) tuvo sus orígenes y validación metodológica en el ámbito de la salud pública. Por mucho tiempo, ha sido utilizado por organizaciones mundiales para lograr medir la efectividad de las campañas de prevención de enfermedades y cambio de hábitos sanitarios. Sin embargo, hoy en día, su uso ha ampliado su alcance al ámbito tecnológico, adoptando la naturaleza fundamental de la teoría del comportamiento para aplicarlo en ciberseguridad.

La academia contemporánea, apoyada en investigaciones robustas como las de Kruger & Kearney (2006) y Hadlington (2017), establece que la seguridad de los datos corre riesgo con una amenaza conductual similar a la defensa de la higiene pública; la responsabilidad individual debe garantizar buenos hábitos digitales para protegerse.

Conocer teóricamente una amenaza como un ataque de *phishing* no garantiza que el usuario tome las medidas preventivas adecuadas en la práctica. Dado que la ingeniería social explota vulnerabilidades psicológicas y malos hábitos, el modelo KAB resulta ser un marco teórico perfectamente transferible e idóneo para estructurar y evaluar programas de concienciación en ciberseguridad.

Para que un programa sea verdaderamente efectivo y logre mitigar el riesgo humano, este modelo propone que la intervención debe operar en tres niveles interconectados que se muestran en la Tabla 4:

Tabla 4- Niveles Modelo KAB

Nivel	Descripción
Conocimiento (K)	Lo que el usuario sabe sobre las amenazas.
Actitud (A)	Cómo percibe el riesgo y su disposición a seguir protocolos de seguridad.
Comportamiento (B)	Las acciones preventivas reales que el usuario aplica, como el uso de contraseñas seguras y el reporte de incidentes.

En el contexto de este proyecto, permite no solo diseñar estrategias de formación precisas, sino medir el cambio conductual a través de interacciones directas del usuario frente a simulaciones de ataques reales.

3.1.4 Estándares Internacionales y Normativa Legal

ISO/IEC 27001 (ISO/IEC, 2022): Estas normativas exigen la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que el control 7.3 señala que todos los empleados y partes interesadas deberán recibir una formación, educación y capacitación adecuada con relación al tema de la seguridad de la información.

En cuanto a este enfoque normativo reconoce que la tecnología por sí sola es insuficiente y que el fortalecimiento de las competencias humanas constituye un requisito formal y auditable dentro de cualquier sistema de gestión robusto.

Ley Orgánica de Protección de Datos Personales (LOPDP): En Ecuador, esta ley exige a las organizaciones y ciudadanos garantizar la confidencialidad y protección de los datos

personales, siendo la concienciación una medida administrativa fundamental para evitar filtraciones, esta ley establece que los responsables y encargados del tratamiento de datos personales deben adoptar las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado, incluyendo la capacitación del personal autorizado para acceder a dicha información.

3.1.5 Propuestas Existentes en Ciberseguridad

A continuación, se detallan las propuestas más relevantes que sirven de referencia para el presente proyecto:

- **Marcos de Referencia Internacionales (NIST y SANS):** Instituciones globales han desarrollado guías de entrenamiento en ciberseguridad, como el marco de la NIST cuyas siglas significan National Institute of Standards and Technology, que enfatiza la necesidad de un aprendizaje continuo y no solo una charla puntual. Asimismo, el modelo de SANS Security Awareness propone que la concienciación debe ser tratada como un cambio de cultura organizacional y no meramente como un requisito de cumplimiento técnico.
- **Iniciativas del Sector Financiero:** La Asociación de Bancos Privados del Ecuador conocido como ASOBANCA ha impulsado campañas de educación financiera digital que incluyen consejos de seguridad básicos, estas propuestas suelen ser de carácter informativo general y carecen de un sistema de medición cuantitativo.

3.2 METODOLOGÍA DE INVESTIGACIÓN

La metodología de este proyecto se desarrolla bajo un enfoque cuantitativo, un diseño cuasi-experimental y un alcance descriptivo-propositivo. Esta estructura metodológica garantiza el rigor técnico necesario para un proyecto de ciberseguridad, permitiendo que la propuesta se sustente en telemetría y datos estadísticos objetivos extraídos de sistemas reales, en lugar de encuestas de autopercepción.

- **Enfoque Cuantitativo:** Cuantificar el nivel de vulnerabilidad real de los usuarios mediante las tasas de interacción con amenazas simuladas, transformar las brechas del modelo KAB en indicadores medibles, validados inferencialmente mediante la Prueba Exacta de McNemar y el Tamaño del Efecto de Cohen.
- **Alcance Descriptivo y Propositivo:** Se caracterizan las debilidades de conducta ante la ingeniería social en la muestra inicial para posteriormente desarrollar un plan de capacitación bajo el formato de microlearning; lo que implica asegurar que cada bloque educativo cubra la vulnerabilidad específica detectada.
- **Diseño Cuasi-experimental:** Se analiza la eficacia de un nuevo modelo a través de una muestra control completa. Para lograr esto, utiliza medidas longitudinales divididas en fase inicial y medición después de la intervención, ambas realizadas dentro del ambiente del usuario.

3.2.1 Métodos Aplicados

Método Analítico: Sirvió para interpretar los datos crudos arrojados por Gophish, aquí se utilizó la Tasa de Apertura solo para confirmar qué usuarios vieron el correo y tomamos las verdaderas acciones de riesgo (los clics, los datos ingresados y los reportes) y se lo vinculó

directamente con las partes del modelo KAB. Esto permitió descubrir qué fallas humanas específicas aumentan el peligro para la empresa y el usuario.

Método Deductivo: Su uso permitió aterrizar la teoría general del comportamiento seguro frente al riesgo digital, adaptándola a la realidad específica de la empresa en el caso piloto. Con esto se aseguró de que la capacitación propuesta tenga una base lógica estructurada y fundamentada, aplicable a cualquier entorno corporativo.

3.2.2 Procesamiento de Datos

El procesamiento y análisis de los datos recolectados se estructuró en dos niveles complementarios para garantizar el rigor científico y la objetividad de los resultados:

- **Descriptivo:** La recolección de métricas iniciales se realizó de forma automatizada mediante la telemetría de la plataforma Gophish, estos datos crudos de interacción fueron extraídos, tabulados y clasificados directamente bajo los parámetros de la Matriz de Riesgo de cuatro niveles Riesgo Bajo, Medio, Alto y Crítico.
- **Inferencial:** Para validar estadísticamente la efectividad del programa de concienciación propuesto y demostrar empíricamente la reducción de la vulnerabilidad en los usuarios, los datos emparejados obtenidos en la prueba piloto fueron sometidos a un análisis inferencial riguroso. Se aplicó la Prueba Exacta de McNemar para evaluar los cambios significativos en el comportamiento dicotómico frente a las amenazas simuladas, complementada con el cálculo del Tamaño del Efecto *h* (Cohen, 1988) para medir la magnitud y relevancia práctica de la intervención educativa, descartando así que las mejoras obtenidas fuesen producto del azar.

3.3 TECNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las técnicas seleccionadas para este estudio permitieron transformar comportamientos humanos cualitativos en indicadores métricos objetivos, facilitando tanto el diagnóstico de la línea base como la posterior validación del programa de concienciación mediante análisis estadístico.

3.3.1 Simulación Automatizada de Ingeniería Social

Como herramienta central de medición se utilizó Gophish, un software de código abierto que permitió evaluar la vulnerabilidad real de los usuarios ante ataques de ingeniería social.

No se realizó encuestas o entrevistas, ya que en esos formatos las personas suelen sobreestimar sus propios conocimientos. En su lugar, se lanzó dos campañas de phishing simulado sin previo aviso para observar cómo reacciona el personal en su día a día.

Con los datos recolectados, se realizó un análisis de riesgo que se construyó cruzando las interacciones reales con las tres áreas del modelo KAB:

- **Conocimiento (K) - Tasa de Clics:** Evaluación de discriminación visual hacia las amenazas. Medirá la deficiencia de los usuarios que no pudieron reconocer las señales de alerta de phishing en el cuerpo del correo y que finalmente presionaron el enlace sospechoso.
- **Actitud - Tasa de Captura de Credenciales:** Se evalúa la percepción de riesgo y la confianza excesiva del usuario, también cuántos usuarios, después de acceder a la página engañosa, olvidaron advertir el riesgo obvio y fueron dispuestos a revelar datos confidenciales.

- **Comportamiento - Tasa de Reporte:** Registra la ejecución (u omisión) de los protocolos de seguridad de la organización. Evalúa si el usuario actuó como un sensor activo de defensa al ejecutar la acción segura de reportar el incidente al área de TI.

Los datos objetivos extraídos del tablero de control (Ver Anexo 1) de esta herramienta constituyen el insumo cuantitativo directo para clasificar el nivel de vulnerabilidad de la muestra mediante la Matriz de Riesgo de 4 Niveles, garantizando la trazabilidad e inmutabilidad de la evidencia recolectada.

3.4 POBLACIÓN Y MUESTRA

En esta sección se describe el grupo humano sobre el cual se fundamenta el estudio y la validación empírica de la propuesta, asegurando que los resultados obtenidos sean representativos del usuario de banca electrónica.

- **Población:** El universo de este estudio comprende a los ciudadanos de Guayaquil que utilizan canales digitales en sus labores cotidianas.
- **Muestra:** Se ha seleccionado una muestra no probabilística por conveniencia de 30 colaboradores pertenecientes a la empresa Heurística S.A. (sucursal Guayaquil). Este grupo funciona como un caso de estudio piloto altamente representativo del ciudadano común.
- **Criterios de Selección:** La muestra integra a usuarios de diversas áreas funcionales operativas y administrativas, excluyendo al personal con conocimientos técnicos avanzados en sistemas, asegurando así una visión real del nivel de resiliencia digital de un usuario promedio.

3.4.1 Consideraciones Éticas y Consentimiento

Para garantizar la integridad, legalidad y ética de la investigación práctica, el proceso se rige bajo los siguientes principios:

- **Autorización Institucional:** El proyecto cuenta con la aprobación formal de la Dirección de Tecnología de Heurística S.A., permitiendo el despliegue de las simulaciones y el registro de incidentes bajo estrictas normas de confidencialidad empresarial (ver Anexo 4).
- **Anonimato y Privacidad:** La plataforma de simulación fue configurada exclusivamente para extraer métricas estadísticas generales, los participantes en el momento apropiado fueron informados de la intervención y en ningún momento se almacenaron permanentemente contraseñas reales, cumpliendo estrictamente con la Ley Orgánica de Protección de Datos Personales (LOPDP).
- **Protocolo de Intervención:** Las simulaciones de ingeniería social se realizaron de forma ciega en dos campañas (Pre-test y Post-test) para medir objetivamente la efectividad de la capacitación.

CAPÍTULO 4

4.1 PROPUESTA

El programa propuesto constituye una respuesta estructurada a las brechas identificadas en la línea base, diseñado específicamente para el perfil del usuario común de servicios financieros digitales, este diseño utiliza una metodología de Microlearning asincrónico. Esta decisión estratégica garantiza la escalabilidad del proyecto, permitiendo que el programa sea implementado masivamente por cualquier institución bancaria o empresa sin depender de instructores presenciales.

4.1.1 Materiales del Programa

Para asegurar una implementación autónoma y estandarizada, el programa se compone de dos kits de materiales:

- **Para el Administrador/Instructor:** Guía de implementación del programa y plantillas de correo estándar para la distribución de los módulos. El diseño modular del programa permite que la medición de efectividad pueda ejecutarse utilizando cualquier plataforma de ciberseguridad que la institución ya posea en su infraestructura, garantizando su total interoperabilidad y facilidad de despliegue.
- **Para el Participante (Usuario Final):** El programa se entrega a través de una aplicación web interactiva estática desarrollada en HTML5 y JavaScript, diseñada bajo el concepto de cero dependencias. Esta arquitectura ligera permite que la institución aloje el contenido en cualquier intranet corporativa sin requerir servidores de backend. El usuario accede a las cápsulas de aprendizaje y, de forma inmediata, el sistema le despliega un Quiz de

validación en el lado del cliente (Frontend) para garantizar la asimilación de los conceptos. (Ver capturas del prototipo interactivo en los Anexos 5, 6 y 7).

4.1.2 Desarrollo de la Propuesta Educativa

La propuesta se estructura en tres módulos de aprendizaje interactivo diseñados con un lenguaje ciudadano. Para facilitar la asimilación por parte del usuario final, las tres dimensiones técnicas del modelo KAB fueron traducidas en la interfaz de la aplicación a tres verbos de acción directa: Saber, Pensar y Actuar. El programa en su totalidad está diseñado bajo la metodología de Micro aprendizaje, requiriendo una inversión de tiempo aproximada de 40 minutos para su finalización y certificación.

Módulo 1: Detectar Correos y Enlaces Falsos (Dimensión K / Saber)

Objetivo: Desarrollar en el usuario la capacidad de reconocer correos y mensajes peligrosos antes de interactuar con ellos.

- **Contenido: Identificación visual**

    1. Cómo identificar un dominio real o un enlace seguro.
    2. Reconocimiento de extensiones de archivos peligrosas (.exe, .bat, .zip).
    3. La psicológica de cómo actúan los atacantes y usan el miedo para forzar el clic.

- **Actividad / Quiz de validación**

    Evaluación interactiva basada donde el participante lee un caso simulado de recepción de correo y debe seleccionar la respuesta que identifica correctamente los factores de riesgo presentes.

Módulo 2: Proteger tu Identidad y tus Cuentas (Dimensión A / Pensar)

Objetivo: Cambiar la actitud de confianza ciega y fomentar una postura de estar prevenido frente a cualquier solicitud de datos sin importar el canal de comunicación.

- **Contenido: Vishing y Smishing**
    1. El protocolo de Cuelgue y Verifique. Aprender que los bancos nunca pedirán códigos o pines de validación por llamada o mensajes.
    2. Autenticación Multifactor (MFA): Aprender por qué una contraseña sola ya no es tan segura y la importancia de activar el múltiple factor de autenticación.
    3. Secuestro de cuentas y suplantación de identidad.
- **Actividad / Quiz de validación:**

  Presentación de escenarios, el participante deberá identificar correctamente los factores de riesgo presentes.

Módulo 3: Cómo Reaccionar ante un Ataque (Dimensión B / Actuar)

Objetivo: Convertir el usuario de una posible victima a un guardia de seguridad dotándolo de un protocolo de acción claro, para mitigar el daño y alertar a la organización.

- **Contenido: Protocolo de acción inmediata**
    1. ¿Qué protocolo seguir si mis contraseñas fueron expuestas?
    2. La importancia del reporte temprano a TI como herramienta de protección colectiva.
    3. Hábitos de seguridad digital como cambio seguro de credenciales.

- **Actividad / Quiz de validación:**

  Resolución de un caso práctico de incidente. El participante debe seleccionar la opción múltiple que describa la secuencia de comportamiento segura y correcta tras haber caído en una estafa.

En la Tabla 5 se puede ver el detalle de los módulos.

Tabla 5 - Estructura Comparativa y Pedagógica de los Módulos

Dimensión	**Temas Centrales**	**Formato y Actividad**	**Aprendizaje**
Conocimiento	Identificación de remitentes, archivos venenosos, urgencia psicológica.	Cápsula interactiva y Quiz.	El usuario podrá identificar vectores de ataque antes de interactuar.
Actitud	Phishing, Múltiple factor autenticación.	Cápsula digital interactiva y Quiz.	Adoptar una postura de cero confianzas y verificar cada interacción.
Comportamiento	Saber a quién llamar y como reportar.	Cápsula digital interactiva y Quiz.	Generar el hábito de ser el primero en actuar ante el peligro.

RESULTADOS

Para evaluar la efectividad real del programa de concienciación en ciberseguridad desarrollado mediante cápsulas interactivas de Microlearning, se ejecutó una segunda campaña controlada y ciega de phishing simulado (Post-test) dirigida a la misma muestra de 30 colaboradores de Heurística S.A.

Para esta segunda intervención se lanzó una campaña de ingeniería social utilizando un escenario y plantilla de correo con un pretexto administrativo diferente a la inicial donde se solicitaba al usuario dar clic e ingresar datos confidenciales (ver Anexo 9), gracias a la funcionalidad de la herramienta para la clonación exacta de la interfaz del CRM corporativo para la página de destino (ver Anexo 10).

Los datos cuantitativos de esta segunda intervención fueron extraídos desde la plataforma Gophish en su apartado de dashboard donde se obtuvo las siguientes métricas finales (ver Anexo 8):

- **Correos electrónicos enviados:** 30 (100 %)
- **Correos abiertos:** 29 (96.67%)
- **Clics en enlaces:** 8 (26.67 %)
- **Datos y contraseñas expuestas:** 3 (10.00 %)
- **Reportados a TI:** 20 (66.67 %)

Además, a las métricas generales, la plataforma permitió capturar datos ingresados por usuarios los cuales fueron credenciales de acceso de cada interacción individual como se evidencia en el Anexo 8 estos datos personales fueron eliminados posteriormente, el sistema registró los metadatos de los usuarios que cayeron en el engaño, identificando el sistema

operativo y la versión del navegador utilizado. Esta capacidad de perfilamiento técnico confirma la idoneidad de la herramienta no solo para medir la tasa de clics, sino para identificar vulnerabilidades en el entorno tecnológico del usuario final.

Para establecer de forma rigurosa la evolución de la seguridad, estos datos operativos se contrastaron directamente frente a la línea base (*Pre-test*) a través de los criterios estandarizados en la Matriz de Riesgo de 4 Niveles:

En la Tabla 6 se puede ver una comparativa propia a partir de telemetría de Gophish.

Tabla 6 - Comparativa de Vulnerabilidad KAB (Pre-test vs. Post-test)

Dimensión KAB	**Métrica de Evaluación (Fallo)**	**Línea Base (Pre-test)**	**Resultados (Post-test)**	**Evolución de la Vulnerabilidad**
Conocimiento (K)	Tasa de Clics	63.33%	26.67%	Reducción de Riesgo Alto a Riesgo Medio
Actitud (A)	Ingreso de Credenciales	26.67%	10.00%	Reducción de Riesgo Medio a Riesgo Bajo
Comportamiento (B)	Omisión de Reporte a TI	96.67%	33.33%	Reducción de Riesgo Crítico a Riesgo Medio

5.1 Análisis de los Resultados y Cambio Conductual

La comparación directa de las métricas del sistema valida de manera empírica la alta efectividad del programa de concienciación diseñado. El análisis cualitativo y cuantitativo de las dimensiones del modelo KAB ofrece los siguientes hallazgos definitivos:

1. **Ruptura de la Confianza Ciega (Dimensión Conocimiento - K):** Si bien las obligaciones de la rutina laboral empujaron a 29 usuarios a abrir el mensaje (96.67 %), solo 8 de ellos interactuaron con el enlace con esto reduciendo la tasa de vulnerabilidad al (26.67 %) y esto evidencia que el Módulo 2 logró instaurar un criterio de escepticismo activo, enseñando al usuario a buscar señales de alerta visuales y detener la cadena de ataque antes de ejecutar la acción del clic.
2. **Mitigación del Evento de Mayor Impacto (Dimensión Actitud - A):** La entrada de contraseñas cayó drásticamente del 26.67 % en la primera intervención hasta un 10.00 % en la segunda, ubicando esta métrica crítica en el Riesgo Bajo (Nivel 1). Esto demuestra un cambio de actitud en la gestión de información sensible ahora el personal mostró haber aceptado completamente los conceptos sobre blindaje de identidad y protección contra factores de autenticación, por lo que rechazaron dar acceso a sus datos personales, incluso cuando ya habían clicado antes.
3. **Activación de Resiliencia Organizacional (Dimensión Comportamiento - B):** El Módulo 3 tuvo un éxito notable en la mejora de tasa de alerta temprana debido a que pasó de un comportamiento casi ningún reporte en la primera intervención a 20 reportes efectivos y verificados en la segunda intervención.

5.2 Análisis Estadístico Inferencial y Prueba de Hipótesis

Para otorgar validez científica de nivel de postgrado a los resultados obtenidos, y demostrar de forma irrefutable que el cambio en la cultura de seguridad de la organización no es una anomalía estadística o un producto del azar, se procedió a realizar un análisis estadístico inferencial enfocado en la métrica de **conocimiento** determinante (Tasa de Clics)

Planteamiento de Hipótesis

- **Hipótesis Nula (H0):** El programa de concienciación en ciberseguridad no genera una reducción estadísticamente significativa en la vulnerabilidad de los usuarios. Las diferencias observadas entre la fase de Pre-test y Post-test son producto del azar ($p \geq 0.05$).
- **Hipótesis Alternativa (H1):** El programa de concienciación en ciberseguridad reduce significativamente la vulnerabilidad de los usuarios ante ataques de ingeniería social bancaria ($p < 0.05$).

5.3 Selección de la Prueba y Nivel de Significancia

Considerando que la investigación evalúa a la misma muestra exacta de 30 colaboradores en dos momentos cronológicos distintos (muestras relacionadas o emparejadas) y el resultado recopilado por la telemetría del software es de naturaleza dicotómica cualitativa (el usuario interactúa con el riesgo o lo evita; es decir: Clic / No Clic), el estándar estadístico aplicable es la **Prueba Exacta de McNemar**. Se estableció para el análisis un nivel de confianza del 95% con un umbral de error máximo permitido de $\alpha = 0.05$.

Para aplicar la Prueba Exacta de McNemar, se estructuró la siguiente tabla de contingencia de 2x2, la cual rastrea el cambio de comportamiento individual de los 30 colaboradores entre el Pre-test y el Post-test respecto a la acción de hacer clic en el enlace malicioso:

En la Tabla 7 se puede ver la tabla de contingencia.

Tabla 7- Tabla de Contingencia (Distribución de Frecuencias Pareadas)

	Post-test: Hizo Clic	**Post-test: NO Hizo Clic**	**Total Pre-test**
Pre-test: Hizo Clic	8 (a)	11 (b)	19
Pre-test: NO Hizo Clic	0 (c)	11 (d)	11
Total Post-test	8	22	30 (N)

La celda (a) representa a los 8 usuarios que hicieron clic en ambas pruebas. La celda (b) es el indicador de éxito pedagógico: 11 usuarios que hicieron clic en el Pre-test, aprendieron la lección y *no* hicieron clic en el Post-test. La celda (c) demuestra que ningún usuario seguro empeoró su comportamiento.

1. Cálculo de la Prueba Estadística de McNemar (Chi-cuadrado) La prueba de McNemar se enfoca exclusivamente en las celdas discordantes (b y c), es decir, en los individuos que cambiaron de comportamiento. La fórmula del estadístico Chi-cuadrado para McNemar es:

$$\text{Chi-cuadrado} = \frac{(b-c)^2}{b+c}$$

Sustituyendo con los valores empíricos obtenidos en la simulación:

$$x^2 = \frac{(11-0)^2}{11+0}$$

$$x^2 = \frac{121}{11} = 11.00$$

Para un estadístico Chi-cuadrado = 11.00 con 1 grado de libertad (df = 1), el valor de significancia asociado es **p = 0.0009**.

2. Cálculo del Tamaño del Efecto (h de Cohen) Para calcular la magnitud del efecto de la intervención educativa, se aplicó la transformación arcoseno de Cohen sobre las proporciones de fallo del Pre-test (p1 = 0.6333) y Post-test (p2 = 0.2667). La fórmula estándar es:

$$h = 2 \times \arcsin(\sqrt{p1}) - 2 \times \arcsin(\sqrt{p2})$$

Sustituyendo los valores:

$$\alpha 1 = 2 \times \arcsin(\sqrt{0.6333}) - 2 \times \arcsin(\sqrt{0.7958}) = 2 \times 0920 = 1.840$$

$$\alpha 2 = 2 \times \arcsin(\sqrt{0.2667}) - 2 \times \arcsin(\sqrt{0.5164}) = 2 \times 0.542 = 1.084$$

$$h = 1.840 - 1.084 = 0.756$$

Los resultados organizados se los puede ver en la Tabla 8.

Tabla 8 - Resultados de la Prueba de Hipótesis y Tamaño del Efecto

Parámetro Estadístico Evaluado	**Valor Numérico Obtenido**	**Interpretación y Criterio Científico**
Muestra de Estudio (N)	30	Colaboradores evaluados en Pre y Post-test.
Proporción de Fallo Pre-test (p1)	0.6333 (63.33%)	Tasa de Clics basal (Línea de partida).
Proporción de Fallo Post-test (p2)	0.2667 (26.67%)	Tasa de Clics final (Post-intervención).

Valor de Significancia (Valor p)	0.0009	Como p < 0.05, se rechaza la Hipótesis Nula (H0).
Tamaño del Efecto (h de Cohen)	0.76	Magnitud de Efecto Grande (Umbral >0.5 medio, >0.8 grande).

5.4 Análisis Estadístico

El valor de significancia calculado arroja un valor p = 0.0009, el cual es ampliamente menor al límite crítico establecido de α = 0.05. Por consiguiente, **se rechaza formalmente la Hipótesis Nula (H0) y se acepta la Hipótesis Alternativa (H1)**. Existe respaldo estadístico contundente para afirmar que la reducción de la tasa de vulnerabilidad es consecuencia directa de la implementación del programa de concienciación.

A este hallazgo se suma el resultado del estadístico *h* de Cohen, cuyo valor de **0.76** se aproxima de forma estricta al umbral crítico de efecto grande. Esto demuestra científicamente que el programa de *Microlearning* interactivo no provocó un cambio numérico circunstancial, sino que causó una alteración profunda, estable y metodológicamente significativa en los hábitos de seguridad y en el comportamiento de defensa digital de los usuarios que integran el ecosistema evaluado.

CONCLUSIONES

Una vez finalizado el desarrollo del presente proyecto de titulación, y habiendo analizado los resultados empíricos y estadísticos de la intervención piloto, se establecen las siguientes conclusiones:

1. **Sobre la Línea Base y la Vulnerabilidad Humana:** Las pruebas iniciales ejecutadas mediante simulaciones de *phishing* demostraron que las herramientas tecnológicas perimetrales son insuficientes para garantizar la seguridad digital de los usuarios, los resultados mostraron un estado inicial de Riesgo Crítico, evidenciado por una alarmante tasa de clics y una ausencia total de protocolos de reporte. Esto confirmó que el eslabón humano es el vector de ataque más vulnerable para un atacante de ingeniería social.
2. **Sobre el Diseño de la Propuesta:** Se puede concluir que el diseño de programas de concienciación basados en el Modelo KAB tuvo resultados representativos positivamente. La estructuración de la capacitación en cápsulas digitales de Microlearning interactivo y desarrolladas bajo una arquitectura web estática de cero dependencias, no solo facilitó la asimilación de conceptos técnicos, sino que dotó al programa de la agilidad y escalabilidad necesarias para ser implementado masivamente en cualquier intranet institucional.
3. **Sobre la Validación y el Cambio Conductual:** La comparación métrica y estadística entre el Pre-test y el Post-test certifica el éxito rotundo del programa. Se logró reducir la vulnerabilidad en la dimensión de conocimiento del 63.33% al 26.67%, y se incrementó significativamente el comportamiento seguro pasando del 3.33% al 66.67%. La organización evolucionó de un estado de vulnerabilidad crítica a un perfil de resiliencia

proactiva, donde los colaboradores dejaron de ser vectores pasivos de riesgo para convertirse en una primera línea de defensa activa y distribuida.

4. **Sobre el Rigor Estadístico de la Propuesta:** La aplicación de la Prueba Exacta de McNemar ($p = 0.0009$) y el cálculo del Tamaño del Efecto de Cohen ($h = 0.76$) permitieron demostrar científicamente que el cambio en el comportamiento de los usuarios no es producto del azar sino que existe evidencia comprobable de que la intervención educativa propuesta generó un impacto profundo y estable, transformando al colaborador de un sujeto pasivo a un sensor capaz de identificar y reportar los ataques de ingeniería social.

RECOMENDACIONES

A partir de los hallazgos y el éxito de la prueba piloto, se plantean las siguientes recomendaciones para la organización y para futuras líneas de investigación:

Implementación a Nivel Corporativo: Dado el alto tamaño del efecto demostrado en la muestra piloto, se recomienda la adopción del programa de Microlearning interactivo y desplegarlo al 100% de la plantilla laboral en las empresas, integrándolo como un requisito obligatorio y certificable en los procesos de inducción de nuevo personal.

Adopción de la Metodología como Estándar de Auditoría: Se recomienda a la academia y a los profesionales de seguridad de la información adoptar la metodología presentada en este trabajo (Simulación Técnica + Matriz de Riesgo de 4 Niveles + Prueba de McNemar) como un marco estandarizado para auditar objetivamente la madurez de la cultura de seguridad corporativa, dejando atrás las encuestas subjetivas de autopercepción.

Simulaciones Continuas: Se sugiere institucionalizar la ejecución de campañas periódicas de ingeniería social como mecanismo de auditoría continua del comportamiento ya que es vital que estas mediciones mantengan un enfoque estrictamente educativo y de refuerzo positivo, reconociendo y recompensando a los usuarios que reportan incidentes proactivamente.

Actualización del Catálogo de Amenazas: Debido a que la ingeniería social es una técnica criminal en constante evolución que está incorporando actualmente el uso de Inteligencia Artificial, los escenarios de simulación y el contenido de las cápsulas de aprendizaje deben ser revisados anualmente. Se debe poner especial énfasis en actualizar los vectores de ataque multicanal altamente efectivos en el entorno local (tales como la clonación de cuentas en

WhatsApp, fraude del código SMS y tácticas de *Vishing*), asegurando que el entrenamiento refleje las amenazas cotidianas más urgentes.

REFERENCIAS

CrowdStrike. (2025). *Informe sobre el panorama de amenazas en América Latina para el 2025* [PDF]. CrowdStrike Holdings, Inc. https://kwfoundation.org/wp-content/uploads/2025/10/LATAM-Regional-Threat-Landscape-Report_es-LA.pdf.pdf

Banco Central del Ecuador. (2024, 29 de febrero). *El número de operaciones con medios de pago electrónicos se triplicó entre 2019 y 2023*. https://www.bce.fin.ec/el-numero-de-operaciones-con-medios-de-pago-electronicos-se-triplico-entre-2019-y-2023/

Kaspersky. (2025, 10 de septiembre). *Ataques con mensajes falsos aumentan 85% en América Latina: más de 1.2 mil millones de casos detectados*. https://latam.kaspersky.com/about/press-releases/ataques-con-mensajes-falsos-aumentan-85-en-america-latina-mas-de-12-mil-millones-de-casos-detectados-kaspersky

Proofpoint. (2024, 21 de mayo). *Voice of the CISO 2024* (comunicado sobre “human error” 74%). https://www.streetinsider.com/Business+Wire/Proofpoint%E2%80%99s+2024+Voice+of+the+CISO+Report+Reveals+that+ThreeQuarters+of+CISOs+Identify+Human+Error+as+Leading+Cybersecurity+Risk/23254531.html

Banco Central del Ecuador. (2024, octubre). Documento estadístico anual de medios de pago electrónicos en Ecuador 2023. https://contenido.bce.fin.ec/documentos/Administracion/snp-DEAMP2024.pdf.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador (2022-2025). https://gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf.

Verizon. (2024). *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/Tfdb/reports/2024-dbir-data-breach-investigations-report.pdf

ISO/IEC. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Lawrence Erlbaum Associates.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.

Gophish. (2024). *Gophish: Open-Source Phishing Framework*. https://getgophish.com/

Asociación de Bancos Privados del Ecuador [ASOBANCA]. (2024). *Campaña de educación y seguridad financiera digital*. https://www.asobanca.org.ec/

National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

SANS Institute. (2024). *SANS Security Awareness Maturity Model*. SANS Security Awareness. https://www.sans.org/security-awareness-training/maturity-model/

ANEXOS

Anexo 1: Telemetría de la Campaña de Simulación de Phishing (Línea Base - Pre-test)

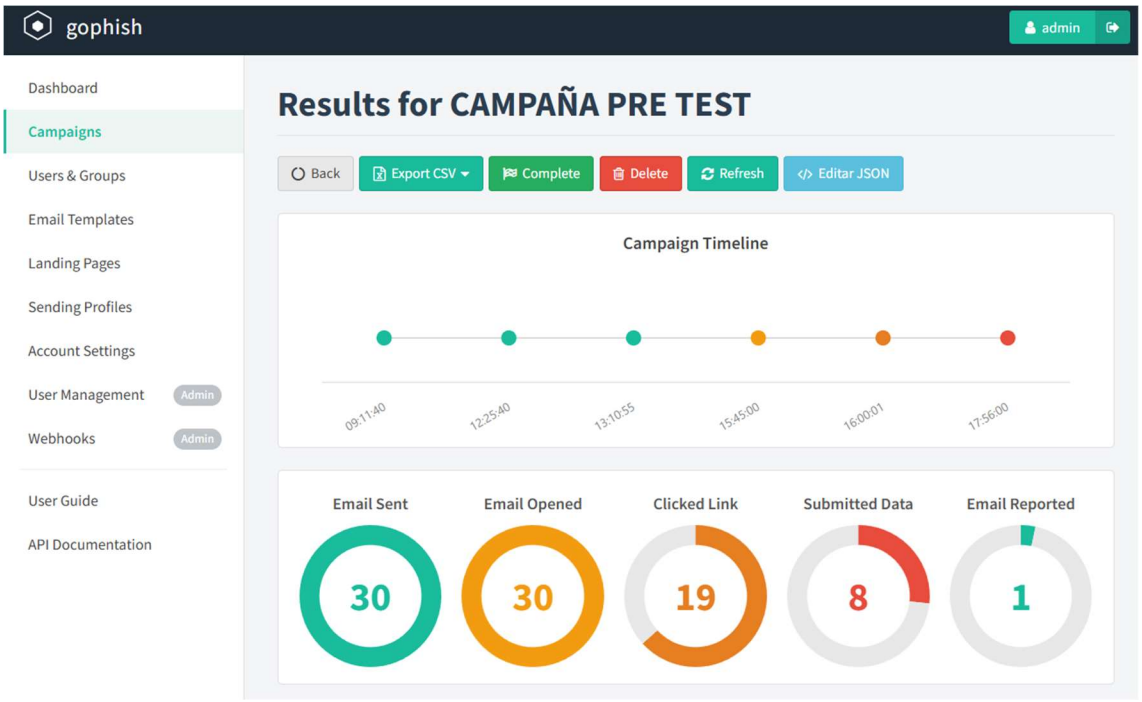

Figura 2- Tablero de control sistema Gophish

Nota: Captura de pantalla del tablero de control de la plataforma Open Source Gophish. En esta sección se evidencian los resultados cuantitativos crudos obtenidos durante el diagnóstico de la línea base (Pre-test).

Anexo 2: Diseño de la Plantilla de Phishing Simulado - Escenario de Urgencia

Figura 3- Plantilla correo campaña inicial

Nota: Captura de pantalla de la plantilla del diseño del correo electrónico configurado y desplegado a través de la plataforma Gophish durante la fase de diagnóstico. El escenario simula una comunicación oficial de la Mesa de Ayuda de la organización, empleando el detonador psicológico de urgencia (advertencia de caducidad de contraseña en 24 horas).

Anexo 3: Diseño de la Página de Captura de Credenciales

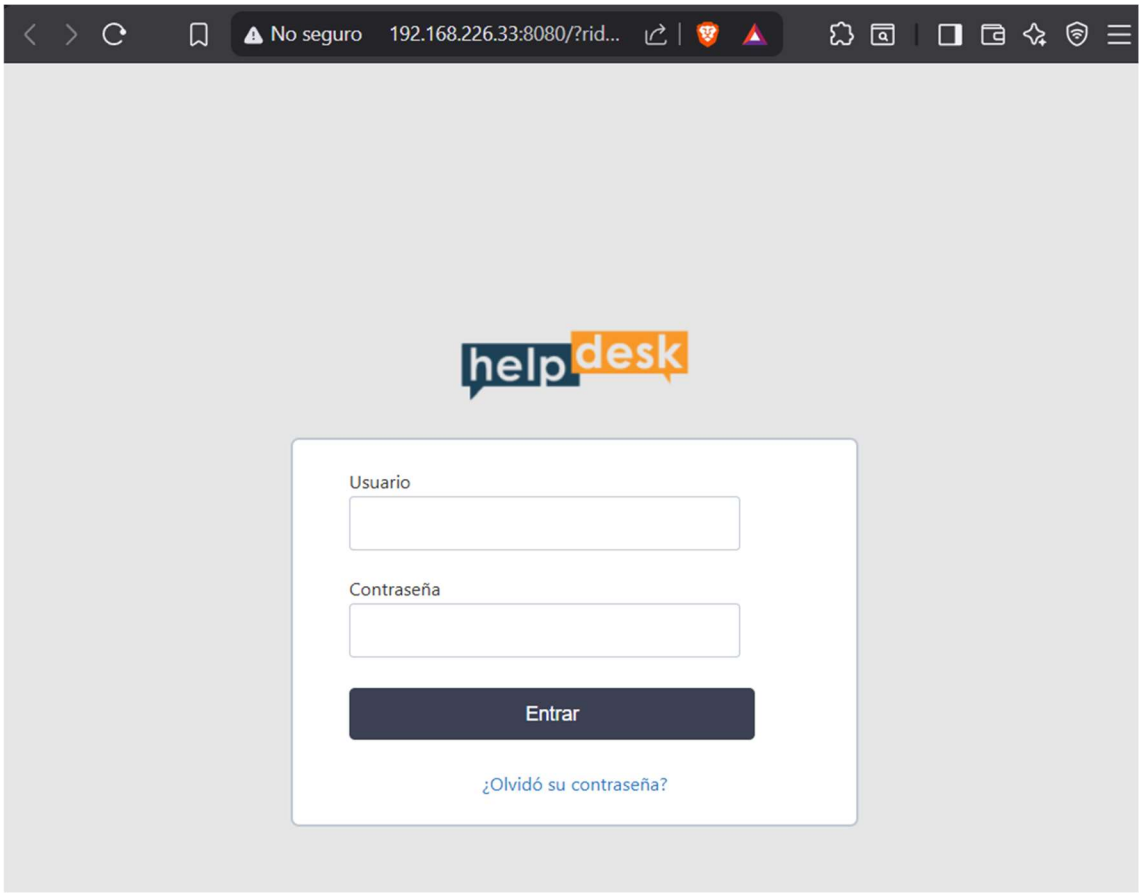

Figura 4 - Diseño página web de captura de credenciales

Nota: Este es un diseño visual que replica el punto de entrada al Servicio de Soporte de la organización. Su propósito metodológico fue medir el Rango (B), tomando en cuenta qué cantidad de usuarios pasó desapercibidos al revisar si la dirección URL era legítima.

Anexo 4: Carta de Autorización Institucional y Consentimiento de Participación.

Guayaquil, 15 de marzo de 2026

Para: Ing. Diego Gaybor
Director de Tecnología
Heurística S.A.

De: Ing. Miguel Angel Mise Chica
Maestrante del Programa de Ciberseguridad
Universidad Estatal Península de Santa Elena (UPSE)

Autorización para la ejecución del proyecto de titulación práctico (Simulación técnica y Programa de Concienciación)

De mi consideración:

Por medio de la presente, solicito formalmente su autorización para llevar a cabo la fase práctica de mi proyecto de titulación de maestría denominado *"Propuesta de programa de concienciación en ciberseguridad para usuarios de banca electrónica en la ciudad de Guayaquil"*. Este proyecto tiene como objetivo evaluar y fortalecer la resiliencia del factor humano frente a ataques de ingeniería social.

ACUERDO DE CONFIDENCIALIDAD Y ANONIMATO

Para proteger la integridad de los colaboradores y de la institución, el investigador se compromete estrictamente a lo siguiente:

- **Anonimato total:** La plataforma *Gophish* será configurada exclusivamente para extraer métricas estadísticas generales (Tasa de Apertura, Tasa de Clics y Tasa de Captura). En ningún momento se registrarán, almacenarán ni expondrán contraseñas reales ni credenciales de los usuarios.
- **Uso académico:** Los datos recolectados serán utilizados con fines netamente académicos y estadísticos.
- **No afectación laboral:** Los resultados obtenidos en las simulaciones no estarán vinculados a evaluaciones de desempeño laboral ni tendrán repercusiones corporativas para los participantes.
- **Cumplimiento legal:** Todo el proceso se enmarcará en el respeto a la confidencialidad empresarial y a la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador.

Agradeciendo de antemano su apertura y apoyo a la investigación académica que beneficiará la postura de seguridad de la organización, suscribimos este documento en conformidad.

Atentamente,

Ing. Miguel Angel Mise Chica
Maestrante en Ciberseguridad – UPSE
Investigador Responsable

APROBACIÓN INSTITUCIONAL:

Por medio de la presente firma, confirmo que he leído los términos expuestos y AUTORIZO la ejecución de las simulaciones en los sistemas/correos designados para la muestra, así como la realización del programa de capacitación en las instalaciones/medios de Heurística S.A.

Ing. Diego Gaybor
Director de Tecnología
Heurística S.A.

DIEGO PATRICIO GAYBOR QUIROZ
Diego Patricio Gaybor Quiroz.
Director de Tecnología

Figura 5 - Carta de autorización

Anexo 5: Interfaz Principal y Tablero de Control

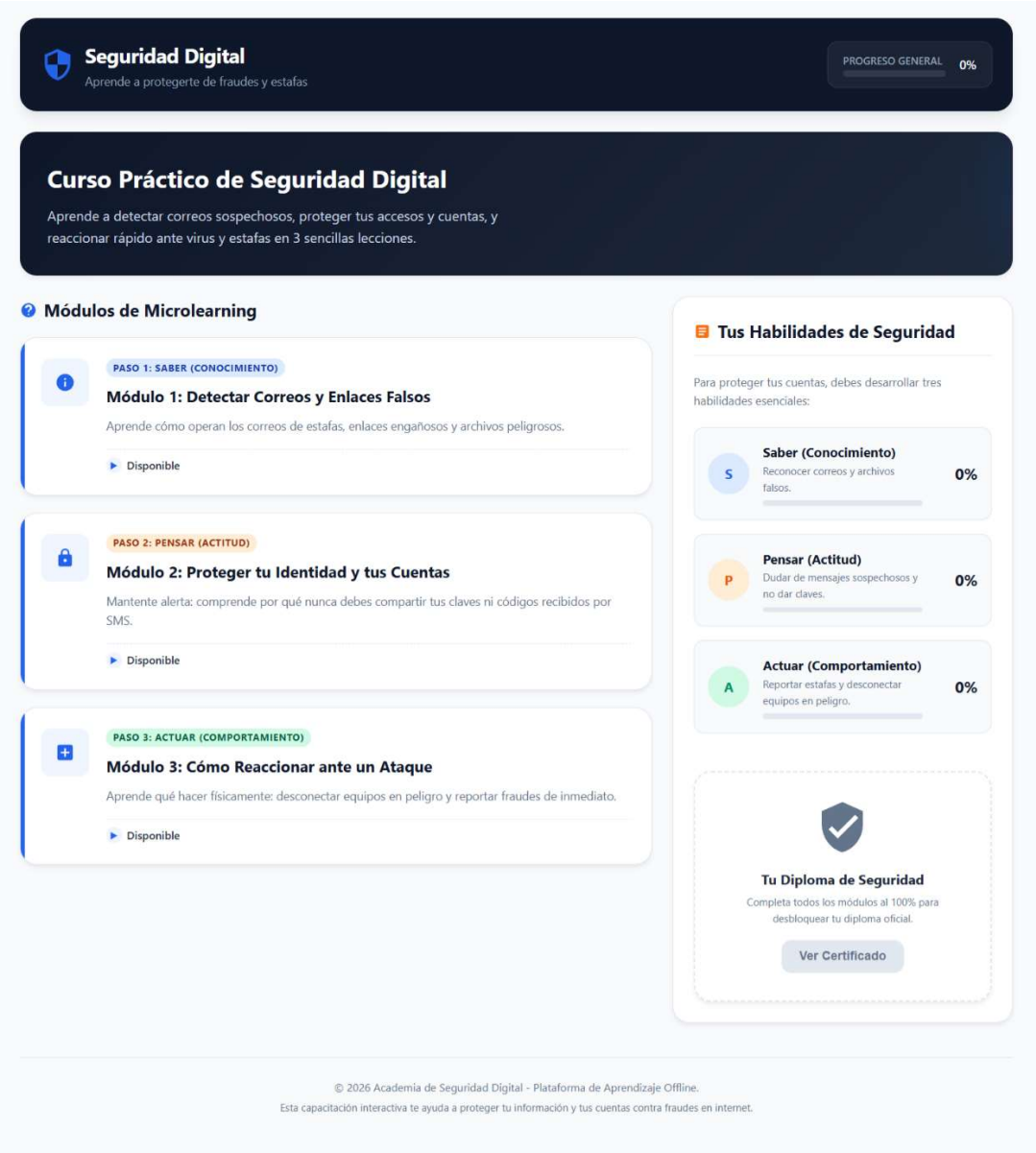

Figura 6 - Interfaz principal programa capacitación

Nota: Captura de pantalla de la interfaz principal de la aplicación web estática (*Single Page Application*). El panel de control permite al usuario visualizar su progreso general y acceder a los tres módulos de *Microlearning* alineados al modelo KAB. El diseño implementa una arquitectura de cero dependencias que garantiza su ejecución local y *offline* en cualquier equipo corporativo.

Anexo 6: Cápsulas de Aprendizaje Interactivo (Modelo KAB)

Pantalla Módulo 1

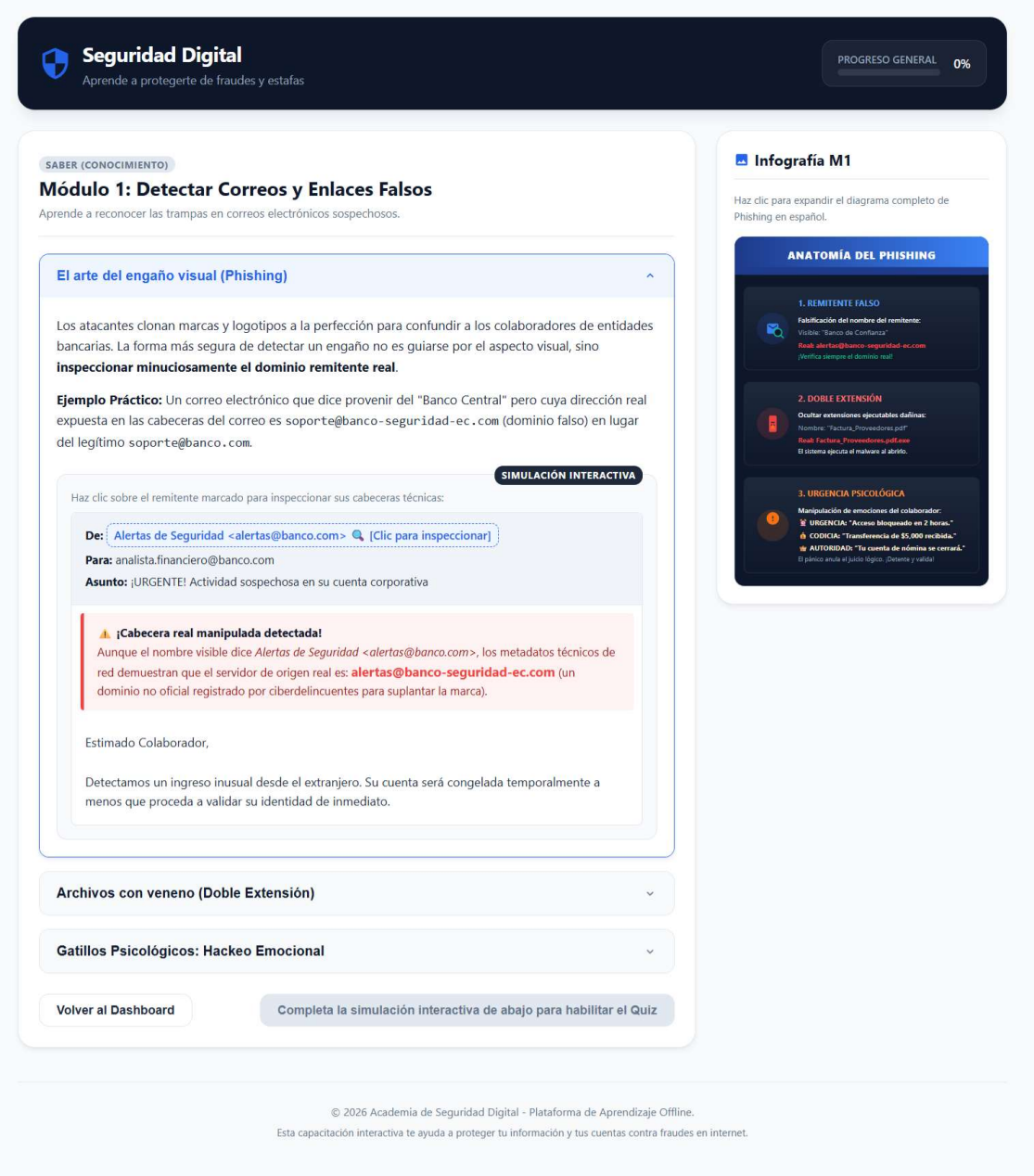

Figura 7- Módulo 1 programa capacitación

Pantalla Módulo 2

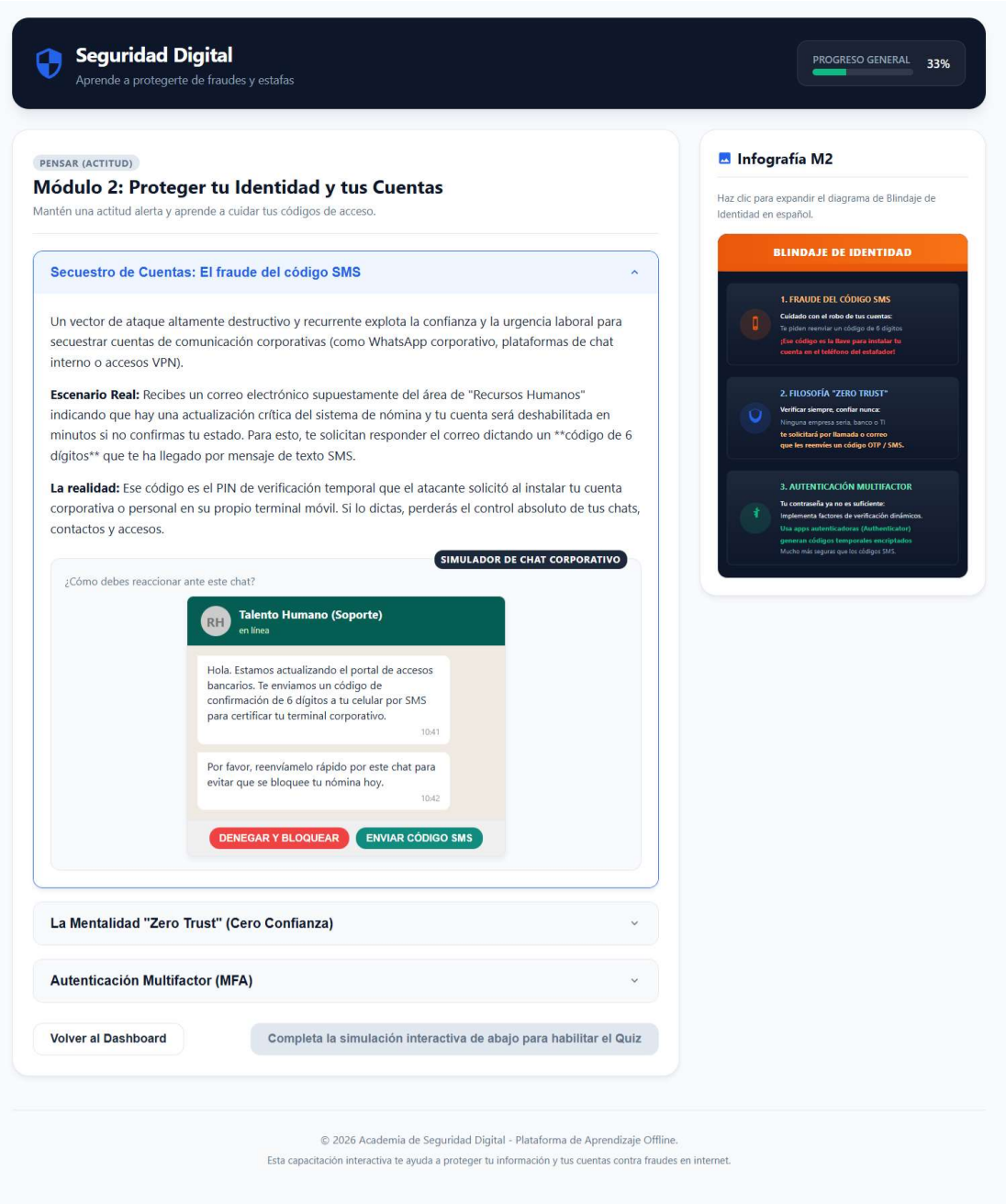

Figura 8 - Módulo 2 programa capacitación

Pantalla Módulo 3

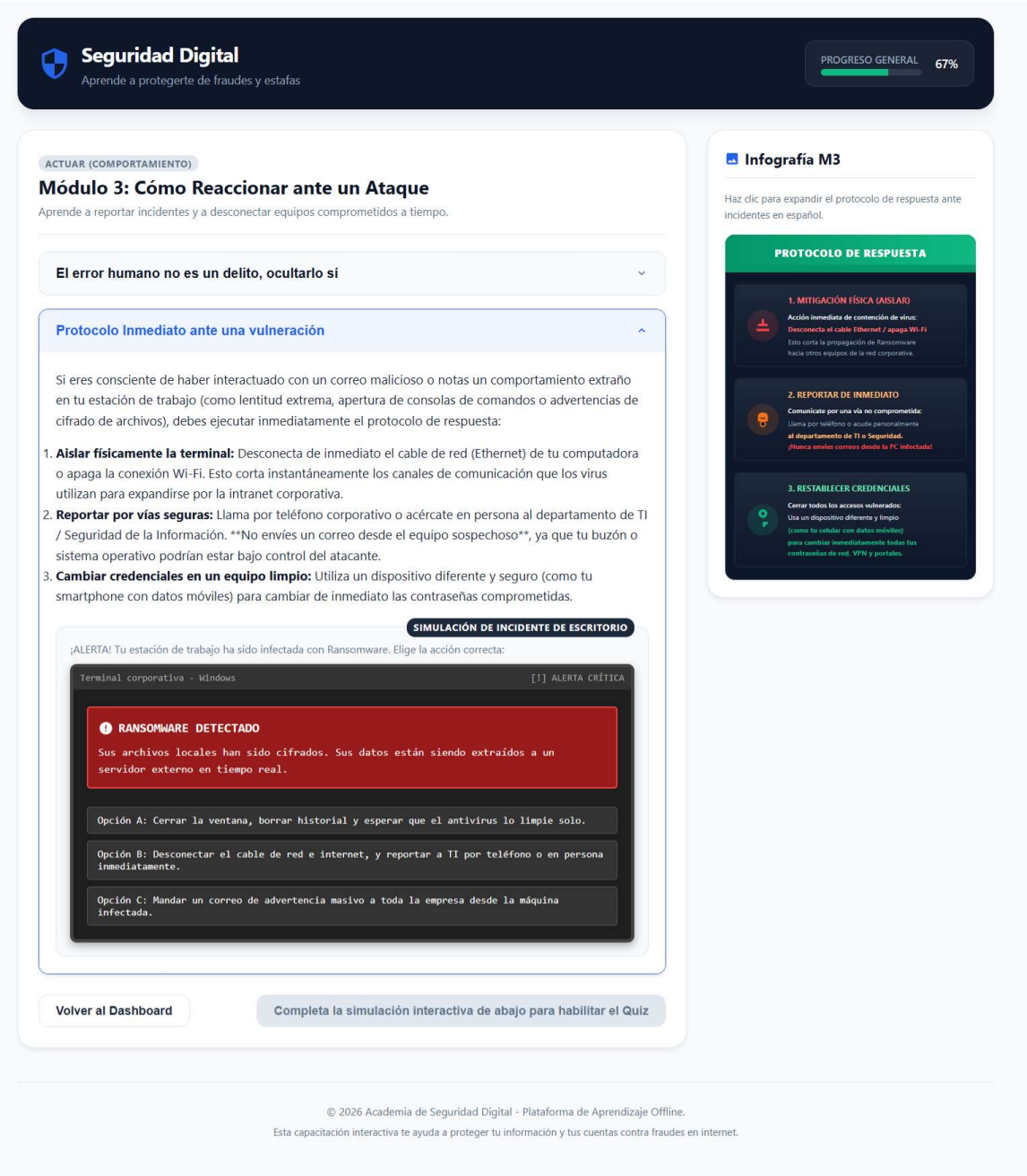

Figura 9 - Módulo 3 programa capacitación

Nota: Vistas del contenido pedagógico de los módulos KAB. Cada cápsula incluye infografías explicativas y simuladores de escritorio interactivos.

Anexo 7: Sistema de Evaluación en el Cliente y Certificación Automática

Pantalla de preguntas de evaluación del módulo

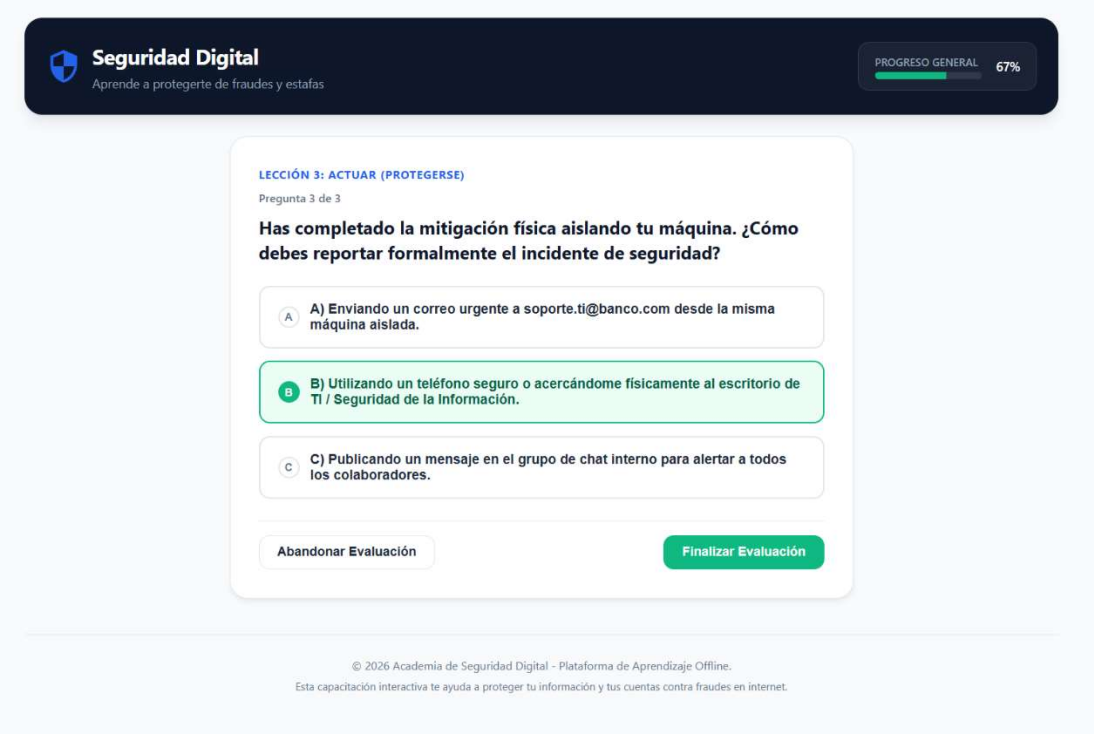

Figura 10 - Interfaz de preguntas programa capacitación

Pantalla de resultados de evaluación

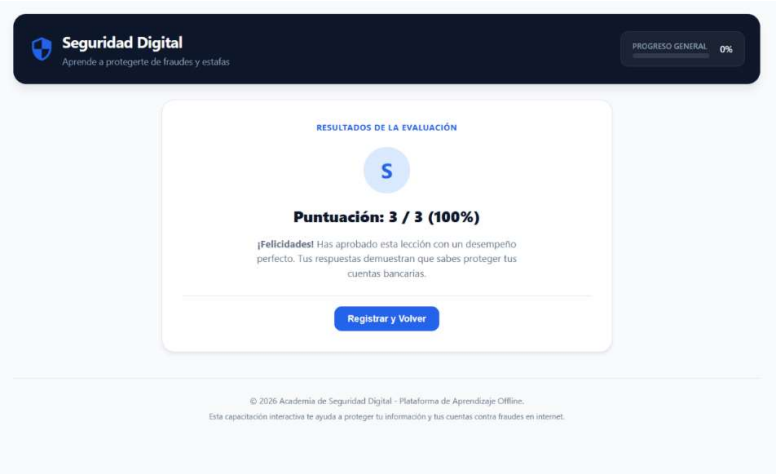

Figura 11 - interfaz de vista de resultados programa capacitación

Pantalla de presentación de diploma de completar el curso.

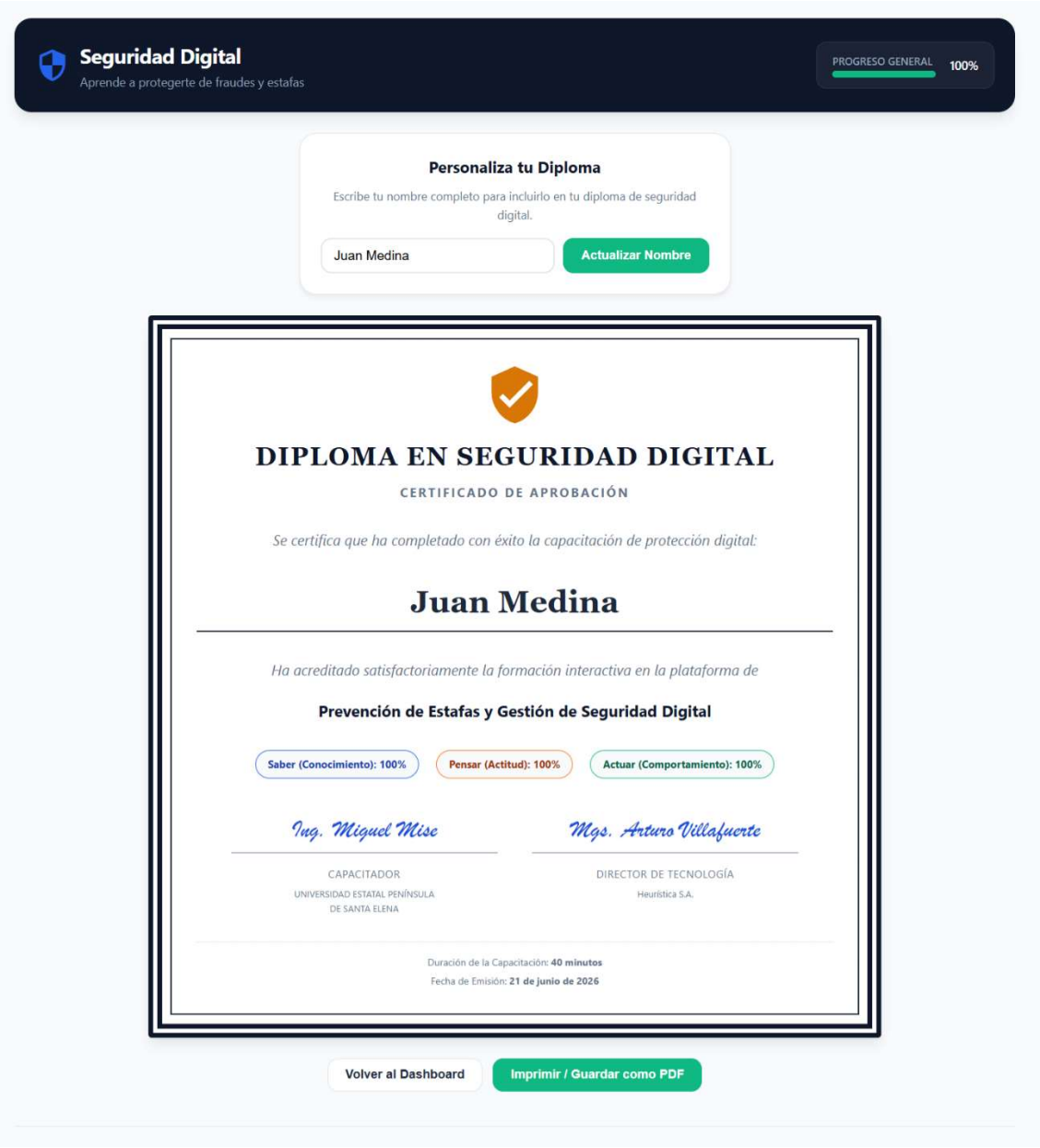

Figura 12 - Certificación de completar el programa de capacitación

Nota: El sistema genera dinámicamente un certificado de aprobación personalizado, listo para ser impreso o guardado en formato PDF como evidencia de cumplimiento normativo para el departamento de Recursos Humanos.

Anexo 8: Telemetría de Resultados - Campaña Post-test (Gophish)

Resultados de la Campaña

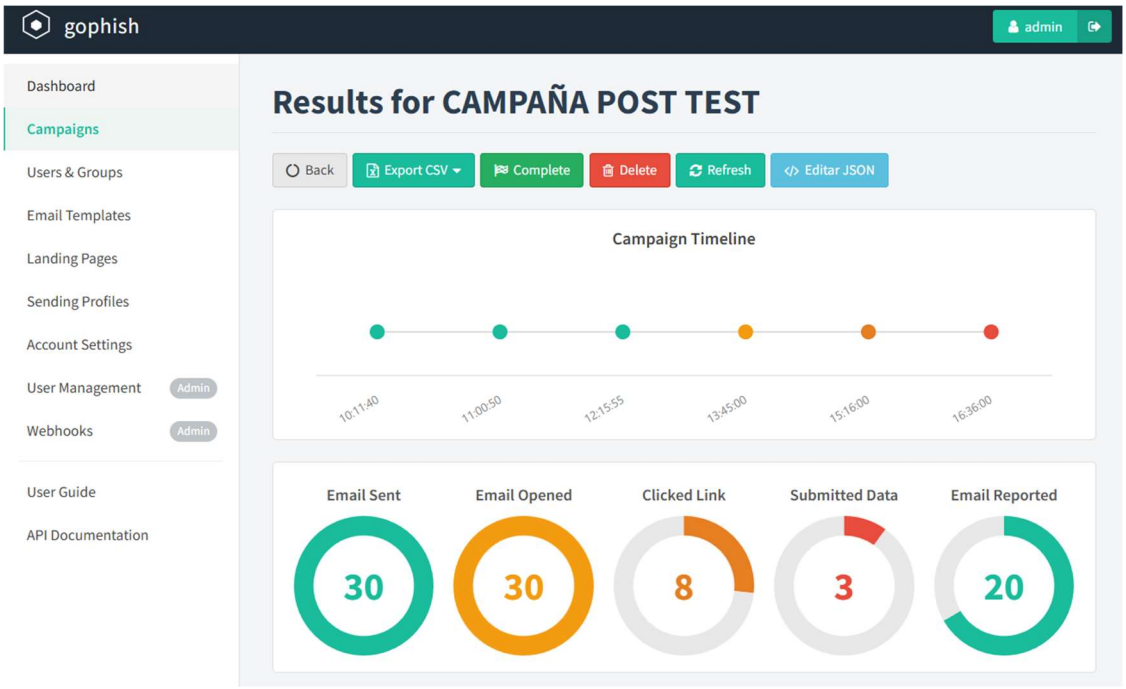

Figura 13 - Resultados de campaña Post Test

Detalle Granular de Interacción por Usuario

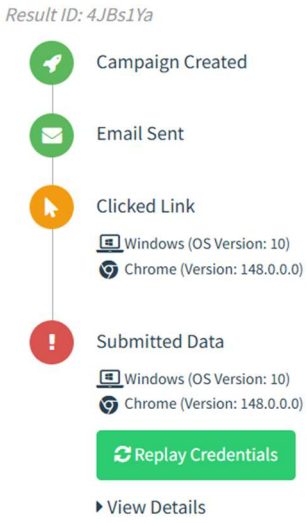

Figura 14 - Evidencia de captura de credenciales

Anexo 9: Diseño de la Plantilla de Phishing Simulado (Post-test) - Escenario Administrativo

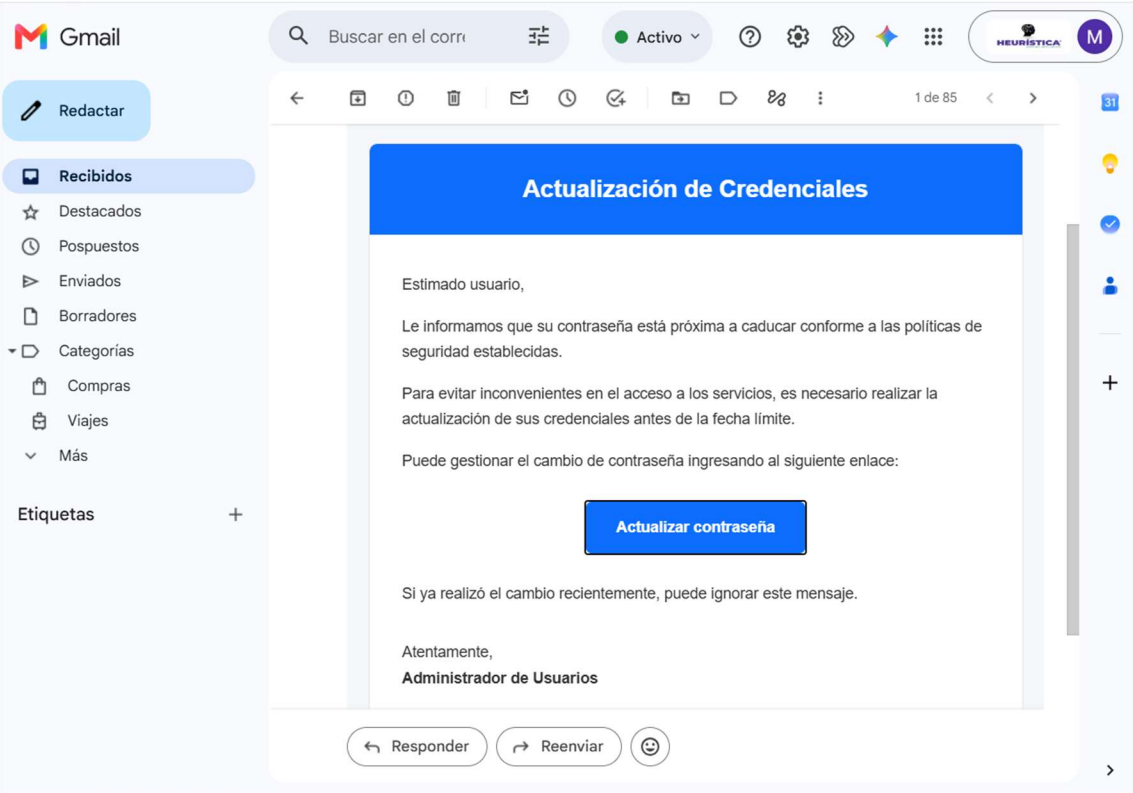

Figura 15 - Diseño plantilla Post Test

Nota: Captura de pantalla del diseño del correo electrónico desplegado durante la fase de Post-test. Para garantizar la validez metodológica y evitar que la reducción en la tasa de clics fuera producto de la memorización del ejercicio anterior, se diseñó un escenario completamente nuevo. Se suplantó la identidad del Administrador de Usuarios exigiendo una actualización de credenciales.

Anexo 10: Diseño de la Página de Captura de Credenciales (Post-test) - Clonación de CRM

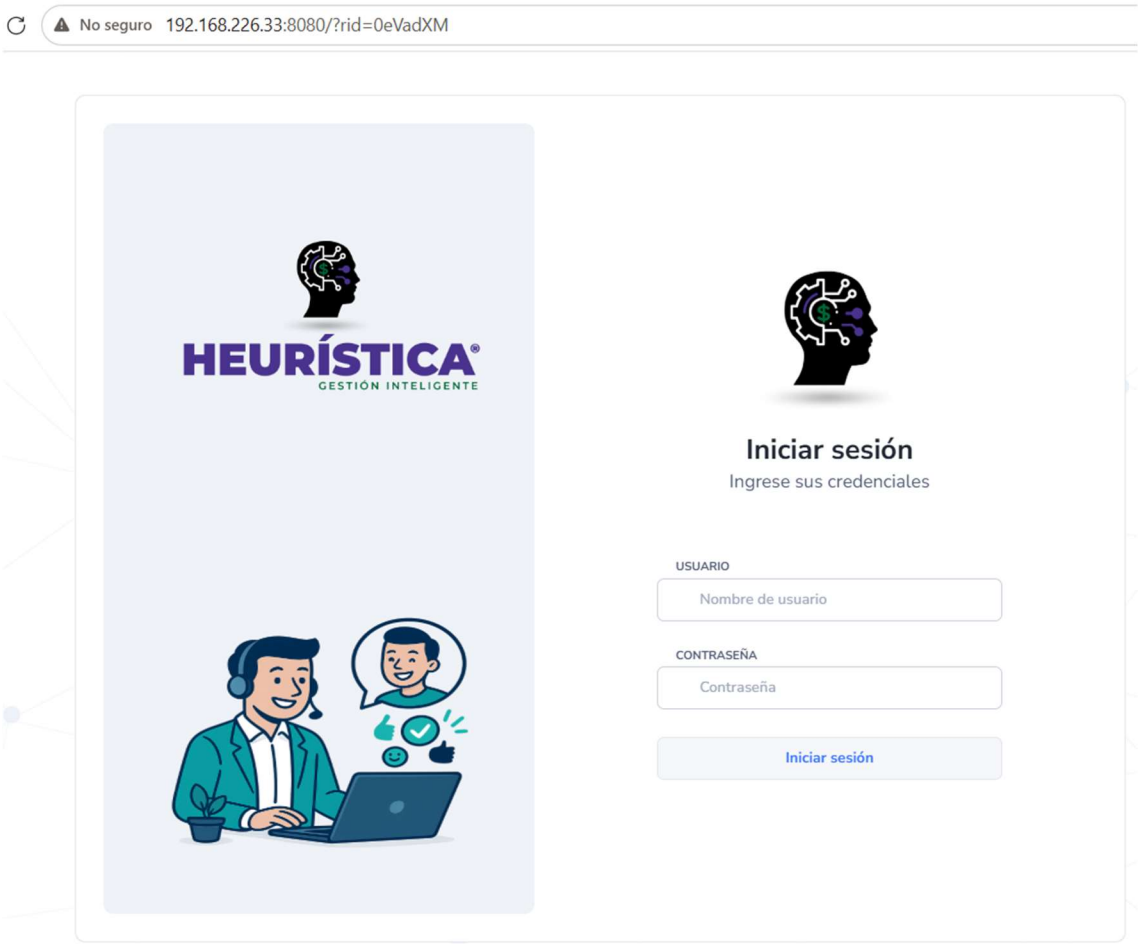

Figura 16 - Diseño página web captura de credenciales Post Test

Nota: Captura de la página de destino utilizada en el Post-test. Utilizando las capacidades de clonación de la plataforma Gophish, se replicó con exactitud la interfaz gráfica del CRM principal de la organización, la efectividad de la capacitación se evidencia en el hecho de que el 90% de los usuarios detectó las señales de alerta visuales expuestas en la barra de direcciones evitando así el compromiso de sus credenciales.