



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

TÍTULO

PROPUESTA DE IMPLEMENTACIÓN DE UN PROGRAMA
PILOTO DE SIMULACIÓN DE ATAQUES DE PHISHING Y
CAPACITACIÓN CORRECTIVA EN LA CIUDAD DE QUITO

AUTOR

Villafuerte Benavides, Arturo Jose

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Cárdenas Cobo, Jesennia del Pilar

**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:
**JESENNIA DEL PILAR
CARDENAS COBO**

**Lcda. Jesennia Cárdenas Cobo, Ph.D.
TUTOR**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**JAIME BENJAMIN
OROZCO IGUASNIA**

**Ing. Jaime Orozco Iguasnia, Mgtr.
DOCENTE
ESPECIALISTA**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**CARLOS EFRAIN
SANCHEZ LEON**

**Ing. Carlos Sánchez León, Mgtr.
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 **VILLAFUERTE BENAVIDES ARTURO JOSE**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR



Validar únicamente en FirmaBC.
Firmado electrónicamente por:
**JESENNIA DEL PILAR
CARDENAS COBO**

Lcda. Jesennia Cárdenas Cobo, Ph.D.

Santa Elena, 21 de Agosto del 2026



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

DECLARACIÓN DE RESPONSABILIDAD

Yo, ARTURO JOSE VILLAFUERTE BENAVIDES

DECLARO QUE:

El Trabajo de Titulación, **"PROPUESTA DE IMPLEMENTACIÓN DE UN PROGRAMA PILOTO DE SIMULACIÓN DE ATAQUES DE PHISHING Y CAPACITACIÓN CORRECTIVA EN LA CIUDAD DE QUITO"**, 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.

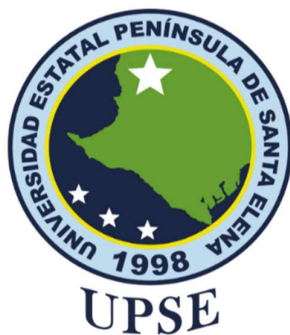
En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 21 de agosto del 2026

EL AUTOR



Villafuerte Benavides Arturo Jose



**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 IMPLEMENTACIÓN DE UN PROGRAMA PILOTO DE SIMULACIÓN DE ATAQUES DE PHISHING Y CAPACITACIÓN CORRECTIVA EN LA CIUDAD DE QUITO”**, presentado por el estudiante, **VILLAFUERTE BENAVIDES ARTURO JOSE** fue enviado al Sistema Anti plagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 8%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis
Compilatio Magister+ | UPSE-ECU

Tesis_Definitiva_Villafuerte - Formato (1) V2 (1)
ID : 5180e559288a47a75bc8fe6f2708ab9a65cdd4c6



8%

Textos sospechosos

Nombre del fichero : Tesis_Definitiva_Villafuerte - Formato (1) V2 (1).txt
Tamaño del archivo original : 284,96 kB
Número de palabras : 6869

Depositante : JESSENIA DEL PILAR CÁRDENAS COBO
Fecha de depósito : 29 de julio de 2026
Tipo de carga : interface
fecha de fin de análisis : 29 de julio de 2026

TUTOR



Validado únicamente en FirmaEC.
Firmado electrónicamente por:
**JESSENIA DEL PILAR
CÁRDENAS COBO**

Lcda. Jesennia Cárdenas Cobo, Ph.D.



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

AUTORIZACIÓN

Yo, VILLAFUERTE BENAVIDES ARTURO JOSE

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 complejo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complejo 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, 21 de agosto del 2026

EL AUTOR



Villafuerte Benavides Arturo Jose

AGRADECIMIENTO

Agradezco profundamente a la Universidad Estatal Península de Santa Elena por brindarme la oportunidad de fortalecer mis conocimientos en el ámbito de la ciberseguridad. A mi tutora, la Dra. Jesennia del Pilar Cárdenas Cobo, Ph.D., por su guía constante, exigencia académica y orientación que hicieron posible la culminación de este trabajo. A mis compañeros de la Maestría en Ciberseguridad, Cohorte II, por compartir experiencias y saberes que enriquecieron mi formación profesional.

A mi familia, por su apoyo incondicional y paciencia durante este proceso de formación. A todos los participantes del programa piloto, cuya colaboración fue fundamental para el desarrollo y evaluación de esta investigación.

ARTURO JOSE VILLAFUERTE BENAVIDES

DEDICATORIA

Dedico este trabajo a mi familia, fuente constante de inspiración y fortaleza. Con su amor y comprensión hicieron posible cada paso de este camino académico. Este logro es tan suyo como mío.

A todos aquellos profesionales que, desde sus organizaciones, trabajan día a día para proteger la información y la privacidad de las personas en el entorno digital. Que este aporte contribuya a construir entornos digitales más seguros en Ecuador y en toda Latinoamérica.

ARTURO JOSE VILLAFUERTE BENAVIDES

INDICE GENERAL

RESUMEN	XII
ABSTRACT.....	XIII
INTRODUCCIÓN	1
CAPÍTULO I	3
1. FUNDAMENTACIÓN.....	3
1.1 ANTECEDENTES	3
1.2 DESCRIPCIÓN DEL PROYECTO	4
1.3 OBJETIVOS DEL PROYECTO	4
1.4 JUSTIFICACIÓN DEL PROYECTO	5
1.5 ALCANCE Y LIMITACIONES DEL PROYECTO	6
CAPÍTULO II	9
2. MARCO TEÓRICO Y METODOLOGÍA	9
2.1 MARCO TEÓRICO.....	9
2.2 METODOLOGÍA DEL PROYECTO	10
CAPÍTULO III.....	14
3. PROPUESTA E IMPLEMENTACIÓN	14
3.1 DISEÑO DEL PROGRAMA PILOTO	14
3.2 CONSIDERACIONES ÉTICAS Y NORMATIVAS.....	17
CAPÍTULO IV.....	18
4. RESULTADOS Y ANÁLISIS.....	18
4.1 RESULTADOS POR PARTICIPANTE	18
4.2 VARIACIÓN DE LOS INDICADORES DE LA VARIABLE DEPENDIENTE	18
4.3 ANÁLISIS DE LOS RESULTADOS	19
4.4 HALLAZGOS COMPLEMENTARIOS	20
4.5 COHERENCIA ENTRE OBJETIVOS, METODOLOGÍA Y RESULTADOS.....	21
4.6 ALINEACIÓN CON ESTÁNDARES INTERNACIONALES.....	21
CAPÍTULO V	22
5. CONCLUSIONES Y RECOMENDACIONES.....	22
5.1 CONCLUSIONES	22
5.2 RECOMENDACIONES	23
REFERENCIAS	25
ANEXOS	28

Anexo 1: Encuesta de Diagnóstico — Variable Dependiente Dimensión Perceptual (Pre-test y Post-test)	28
Dimensión 1: Conocimiento sobre phishing	28
Dimensión 2: Percepción de riesgo	28
Dimensión 3: Comportamientos de seguridad	29
Anexo 2: Guía de Entrevista (Post-test — Complemento cualitativo).....	29
Anexo 3: Cronograma de Implementación del Programa Piloto	30

Índice de Tablas

Tabla 1 - Estándares y Marcos de referencia del programa piloto.....	10
Tabla 2 - Diseño cuasiexperimental del estudio	11
Tabla 3 - Métodos de investigación aplicados.....	11
Tabla 4 - Población y muestra del estudio.....	12
Tabla 5 - Técnicas e instrumentos de recolección de datos.....	12
Tabla 6 - Modelo conceptual del programa piloto de simulación con retroalimentación correctiva	14
Tabla 7 - Contenido y características de los módulos de retroalimentación correctiva	16
Tabla 8 - Resultados por participante — Variable dependiente (dimensiones conductual, perceptual y reactiva)	18
Tabla 9 - Comparación de indicadores VD (Pre vs. Post intervención).....	18
Tabla 10 - Mapa de coherencia interna del estudio.....	21
Tabla 11 - Cumplimiento de estándares internacionales	21
Tabla 12 - Cronograma del programa piloto	30

RESUMEN

El presente trabajo evalúa, mediante un diseño cuasiexperimental de pretest y post-test con un solo grupo, la efectividad de un programa piloto de simulación de ataques de phishing con retroalimentación correctiva en cinco usuarios de una organización privada ubicada en la ciudad de Quito, Ecuador. Ante el alarmante incremento de ataques de ingeniería social —Ecuador registró 12,2 millones de intentos de phishing bloqueados en 2023 (Kaspersky LATAM, 2023)— y la brecha existente en programas prácticos de concienciación, se diseñó una intervención de enfoque predominantemente cuantitativo.

La variable independiente es el programa piloto de simulación con retroalimentación correctiva; la variable dependiente es la vulnerabilidad frente a ingeniería social, operacionalizada en tres dimensiones: conductual (tasa de clics en enlaces fraudulentos, TCF), perceptual (encuesta Likert, PEL) y reactiva (tasa de reporte de correos sospechosos, TRC).

Dada la naturaleza piloto del estudio y el tamaño reducido de la muestra, los resultados se consideran preliminares y se sugiere replicarlo en muestras más amplias y diversas ya que la viabilidad y potencial de efectividad del programa de intervención tiene un contexto altamente controlado.

Palabras clave: phishing, ciberseguridad, ingeniería social, retroalimentación correctiva, diseño cuasiexperimental, evidencia preliminar.

ABSTRACT

This study evaluates, through a quasi-experimental one-group pretest–posttest design, the effectiveness of a pilot phishing attack simulation program with corrective feedback among five users of a private organization located in Quito, Ecuador. In light of the alarming increase in social engineering attacks —Ecuador recorded 12.2 million blocked phishing attempts in 2023 (Kaspersky LATAM, 2023)— and the existing gap in practical awareness programs, an intervention with a predominantly quantitative approach was designed.

The independent variable is the pilot simulation program with corrective feedback; the dependent variable is vulnerability to social engineering, operationalized across three dimensions: behavioral (click rate on fraudulent links, CRF), perceptual (Likert-scale survey, PLS), and reactive (suspicious email reporting rate, SRR).

Given the pilot nature of the study and the small sample size, the results are considered preliminary, and replication with larger and more diverse samples is recommended, since the feasibility and potential effectiveness of the intervention program were established within a highly controlled context.

Keywords: phishing, cybersecurity, social engineering, corrective feedback, quasi-experimental design, preliminary evidence.

INTRODUCCIÓN

Actualmente en la era de la transformación digital acelerada, las organizaciones enfrentan varias amenazas cibernéticas que se encuentran en constante evolución. El phishing — técnica de ingeniería social que busca engañar a los usuarios para que revelen información confidencial o ejecuten acciones no autorizadas— este método se ha consolidado como el principal ataque inicial en incidentes de seguridad a nivel global. Según el informe IBM Cost of a Data Breach 2024, el costo promedio de una brecha de seguridad originada por phishing asciende a USD 4,88 millones.

Ecuador no es ajeno a esta problemática. En 2023, los intentos de phishing en el país se sextuplicaron, alcanzando 12,2 millones de ataques bloqueados, ubicando a Ecuador como el quinto país a nivel mundial en detección de phishing (Kaspersky LATAM, 2023). La ciudad de Quito, como principal centro económico del país, concentra la mayor proporción de organizaciones expuestas a este tipo de amenazas.

Aun cuando contamos con la existencia de marcos normativos como la Ley Orgánica de Protección de Datos Personales (LOPD) y estándares internacionales como ISO/IEC 27001:2022, varias organizaciones ecuatorianas no cuentan con programas efectivos de concienciación en ciberseguridad. La capacitación teórica o videos informativos que tradicionalmente se entregan en dichas organizaciones se ve insuficiente para cambiar los comportamientos de los usuarios frente a amenazas actuales de phishing.

Ante esta problemática, el presente trabajo evalúa e identifica la efectividad de un programa piloto que combina simulaciones controladas de ataques de phishing con módulos de retroalimentación correctiva inmediata. Para esto se emplea un diseño

cuasiexperimental de pretest y post-test con un solo grupo con enfoque principalmente cuantitativo. Se plantea la siguiente hipótesis de investigación:

H1: La implementación de un programa de simulación de phishing con retroalimentación correctiva se asocia con una reducción en la vulnerabilidad de los usuarios frente a ataques de ingeniería social, evidenciada por una tendencia favorable en los indicadores TCF, PEL y TRC.

La estructura de este trabajo comprende de cinco capítulos.

- El Capítulo I presenta la fundamentación, antecedentes y objetivos.
- El Capítulo II desarrolla el marco teórico y la metodología cuasiexperimental.
- El Capítulo III detalla el diseño e implementación del programa piloto y su componente de retroalimentación correctiva.
- El Capítulo IV expone los resultados y el análisis de la variable dependiente.
- El Capítulo V presenta las conclusiones, limitaciones y recomendaciones.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

Una de las amenazas cibernéticas más antiguas es el phishing en el mundo digital. Apareciendo por primera vez en la década de 1990, esta técnica de ingeniería social ha evolucionado significativamente en sofisticación y alcance. En el año 2024 representa el 36 % de todas las violaciones de datos en todo el mundo, constituyendo el principal vector de acceso inicial para ciberataques de mayor envergadura (IBM, 2024).

En Latinoamérica, el panorama de amenazas digitales se ha deteriorado rápidamente. Según Kaspersky LATAM (2023), los ataques de phishing en la región se sextuplicaron durante 2023, Ecuador ocupa una posición crítica. El informe SOCRadar LATAM Threat Landscape Report 2024 señala que la combinación de alta conectividad digital y baja cultura de ciberseguridad convierte a los países andinos en blancos preferidos y frecuentes para los atacantes, este escenario no solo refleja un crecimiento acelerado de riesgos sino también una necesidad urgente de fortalecer las buenas proactivas para combatir estas técnicas de ataque.

En el ámbito local de Ecuador el crecimiento acelerado del comercio electrónico ha ampliado de manera significativa la superficie de ataque: el estudio "Ecommerce 2025: VII Medición" (CECE & UEES) reporta más de 81 millones de transacciones digitales en 2024. La LOPDP (2021) y su reglamento (Decreto 904/2023) establecen obligaciones de seguridad para los responsables del tratamiento de datos personales.

Sin embargo, su adopción efectiva en entornos corporativos quiteños está muy limitada actualmente. Estudios académicos recientes como los de León Naranjo et al.

(2025) y Paucar Cordova (2025) confirman que el factor humano sigue siendo el eslabón más vulnerable en la cadena de seguridad.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto consiste en el diseño, implementación y evaluación de un programa piloto de simulación de ataques de phishing combinado con módulos de retroalimentación correctiva inmediata (just-in-time training), aplicado a un grupo de cinco usuarios de una organización privada ubicada en la ciudad de Quito. El programa se llevó con un diseño cuasiexperimental de pre-test y post-test con un solo grupo, mismo que se estructura en tres fases: diagnóstico inicial, intervención y evaluación final.

La retroalimentación correctiva constituye parte esencial del programa de intervención (variable independiente) y no un objetivo independiente del estudio. Su propósito es generar cambios en la variable dependiente (reducción de la vulnerabilidad frente a phishing), para evaluar este impacto se utilizará indicadores específicos TCF, PEL y TRC.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 Objetivo General

Evaluar la efectividad de un programa piloto de simulación de ataques de phishing con retroalimentación correctiva en la reducción de la vulnerabilidad frente a ingeniería social en usuarios de una organización en la ciudad de Quito.

1.3.2 Objetivos Específicos

- Diagnosticar el nivel inicial de vulnerabilidad frente a ataques de phishing y la percepción de riesgo en los participantes, mediante instrumentos cuantitativos y métricas objetivas de simulación.

- Diseñar escenarios de simulación de ataques de phishing que se adapten al contexto organizacional, ajustados según los niveles de complejidad establecidos en el NIST Phish Scale y las directrices CISA Phishing Guidance (2023).
- Implementar el programa de intervención sustentado en simulación de phishing con retroalimentación correctiva inmediata, asegurando que se encuentre alineado con el Control 6.3 de ISO/IEC 27001:2022.
- Evaluar cómo cambian los indicadores de la variable dependiente (TCF, PEL y TRC) antes y después de la intervención, utilizando análisis estadístico descriptivo y apoyándose en el Alfa de Cronbach como referencia exploratoria de consistencia interna.

1.4 JUSTIFICACIÓN DEL PROYECTO

La justificación del presente proyecto se sustenta en tres dimensiones complementarias: técnica, normativa y social.

Desde la perspectiva técnica, el phishing continúa siendo el vector de ataque más prevalente y costoso a nivel global. Los datos del IBM Cost of a Data Breach Report 2024 indican que el costo promedio de una brecha originada por phishing asciende a USD 4,88 millones por empresa. El Informe de Deloitte sobre el Estado Actual de la Ciberseguridad Ecuador 2023 evidencia que la mayoría de las organizaciones ecuatorianas y asea privadas o públicas no cuenta con programas estructurados de simulación.

Según la perspectiva normativa, tanto la LOPDP (Decreto 904/2023) como la ISO/IEC 27001:2022 (Control 6.3) señalan obligaciones explícitas de concienciación y

formación en seguridad. Este proyecto apoya directamente al cumplimiento de estos requisitos normativos, ya que propone un modelo replicable de programa piloto alineado a los estándares internacionales.

Desde el lado social, según investigaciones de Barrera et al. (2024) y Meléndez et al. (2024) confirman que la retroalimentación contextualizada basada en experiencias simuladas es más efectiva que los enfoques únicamente teóricos para cambiar comportamientos que generan riesgo. El proyecto genera que a través de experiencias practicas las personas adopten y mantengan mejor los buenos hábitos de seguridad.

1.5 ALCANCE Y LIMITACIONES DEL PROYECTO

El proyecto abarca el diseño, implementación y evaluación de un programa piloto en un grupo de cinco usuarios de una organización privada ubicada en la ciudad de Quito, durante cuatro semanas. El alcance funcional incluye:

- Diseño y aplicación de la encuesta de diagnóstico pre-intervención (Escala Likert de 5 puntos, 15 ítems).
- Se diseñarán y ejecutarán dos simulaciones de phishing por participante ajustadas según el NIST Phish Scale en niveles alto medio y alto.
- Implementación de módulos de retroalimentación correctiva que se activaran automáticamente después de cada interacción detectada.
- Se aplica una encuesta después de su intervención, los resultados se analizarán mediante estadística descriptiva de los indicadores de la variable dependiente.
- Informe de resultados mediante un documento que presente hallazgos y recomendaciones para escalar el programa.

Limitaciones del estudio

El presente estudio presenta las siguientes limitaciones que deben tomarse en cuenta al interpretar los resultados:

- **Tamaño muestral reducido ($n = 5$):** La muestra corresponde el 16,7 % de la población disponible (30 personas). Esto se justifica porque el estudio tiene carácter piloto, orientado a validar el protocolo antes de escalarlo. Los hallazgos deben entenderse como evidencia preliminar y tendencias observadas, más no como resultados estadísticamente generalizables.
- **Justificación de los cinco participantes:** Se eligieron cinco personas —en lugar de los 15-20 metodológicamente viables— por tres razones: (1) el objetivo es validar el protocolo del programa piloto; (2) el diseño cuasiexperimental con un solo grupo es de naturaleza exploratoria; y (3) el tamaño reducido permitió un seguimiento individualizado y retroalimentación correctiva personalizada.
- **Ausencia de grupo control:** El diseño $O1 \rightarrow X \rightarrow O2$ permite observar cambios en los indicadores, pero no permite establecer una causalidad fuerte. Es decir que no se puede descartar factores externos o el efecto de sensibilización derivado de la participación en las simulaciones.
- **Efecto de sensibilización:** Los participantes sabían que formaban parte de un programa de evaluación, lo que podría haber modificado sus comportamientos de forma independiente a la intervención.

- Alfa de Cronbach como referencia exploratoria: Con $n = 5$ participantes, los valores obtenidos no pueden interpretarse como evidencia estadística robusta. Se requiere $n \geq 20$ para validaciones más sólidas.

CAPÍTULO II

2. MARCO TEÓRICO Y METODOLOGÍA

2.1 MARCO TEÓRICO

2.1.1 Phishing: Definición y Evolución

El phishing es una técnica de ingeniería social mediante la cual un atacante suplanta la identidad de una entidad legítima con el objetivo de engañar a las víctimas para que divulguen información confidencial. El término deriva del inglés "fishing" (pescar), aludiendo a la metáfora de lanzar anzuelos para atrapar víctimas desprevenidas (Barrera et al., 2024).

Los ataques han evolucionado desde correos masivos y genéricos hasta variantes actuales de spear phishing que utilizan información personalizada para crear mensajes altamente convincentes. El uso de inteligencia artificial generativa ha potenciado adicionalmente su sofisticación (Martí Ramírez, 2025; Microsoft, 2025). Según CISA/NSA/FBI/MS-ISAC (2023), los ataques se clasifican en: phishing masivo, spear phishing, whaling, vishing y smishing. Para el presente estudio, el enfoque se centra en el phishing por correo electrónico.

2.1.2 Ingeniería Social y el Factor Humano

La ingeniería social explota principios psicológicos como la autoridad, la urgencia, el miedo, la reciprocidad y la escasez (Cialdini, 2001). El informe Verizon Data Breach Investigations Report 2024 confirma que el factor humano está presente en más del 74 % de todas las brechas de seguridad. La susceptibilidad al phishing está relacionada con el estrés cognitivo, la sobrecarga de información y el contexto emocional (Somesha & Pais, 2022).

2.1.3 Estándares y Marcos de Referencia

Tabla 1 - Estándares y Marcos de referencia del programa piloto

Estándar / Marco	Requerimiento Aplicado	Relación con el Programa Piloto
ISO/IEC 27001:2022 — Control 6.3	Concienciación, educación y formación en seguridad para todos los colaboradores.	Módulos de retroalimentación correctiva y encuesta Likert pre/post.
NIST Phish Scale (NIST TN 2276)	Categorización de dificultad de detección de correos simulados.	Calibración de Simulación 1 (Nivel Medio) y Simulación 2 (Nivel Alto).
CISA Phishing Guidance (2023)	Controles humanos: retroalimentación basada en simulaciones.	Metodología de retroalimentación correctiva inmediata.
LOPDP — Decreto 904/2023	Medidas organizativas de protección de datos y formación del personal.	Consentimiento informado y confidencialidad de datos.

2.1.4 Programas de Simulación y Retroalimentación Correctiva

Los programas de simulación de phishing con retroalimentación correctiva han demostrado ser una de las intervenciones más efectivas para reducir la vulnerabilidad humana. La literatura académica reciente documenta reducciones observadas de entre el 30 % y el 70 % en las tasas de clics tras intervenciones de este tipo (Timko et al., 2024; Karim et al., 2023).

La retroalimentación correctiva —just-in-time training— consiste en proveer materiales educativos inmediatamente después de que un usuario interactúa con un correo simulado, aprovechando el estado de alerta emocional del momento para maximizar la retención del aprendizaje (León Naranjo et al., 2025). Constituye un componente de la variable independiente, no un objetivo del estudio.

2.2 METODOLOGÍA DEL PROYECTO

2.2.1 Tipo y Diseño de Investigación

El presente estudio adopta un diseño cuasiexperimental de tipo pre-test y post-test con un solo grupo, de enfoque predominantemente cuantitativo, orientado a evaluar la variación en la variable dependiente tras la aplicación de la variable independiente. Se declara un enfoque predominantemente cuantitativo dado que los indicadores principales de la VD son métricas objetivas (TCF y TRC) y una escala Likert (PEL).

Tabla 2 - Diseño cuasiexperimental del estudio

Componente	Definición
Variable Independiente (VI)	Programa piloto de simulación de phishing con retroalimentación correctiva inmediata.
Variable Dependiente (VD)	Vulnerabilidad frente a ingeniería social (tres dimensiones).
Dimensión conductual	Tasa de clics en enlaces fraudulentos (TCF) — GoPhish.
Dimensión perceptual	Puntuación media encuesta Likert (PEL) — Google Forms.
Dimensión reactiva	Tasa de reporte de correos sospechosos (TRC) — GoPhish.
Diseño	Cuasi-experimental $O1 \rightarrow X \rightarrow O2$ (un solo grupo, sin grupo control).
Enfoque	Predominantemente cuantitativo.

2.2.2 Métodos de Investigación

Tabla 3 - Métodos de investigación aplicados

Método	Descripción y Aplicación
Inductivo	A partir de los resultados observados en el grupo piloto se generan conclusiones orientadas a contextos organizacionales similares.
Analítico	Se descomponen los datos de clics, encuestas Likert y reportes para identificar patrones de variación en la VD.
Hipotético-Deductivo	Se contrasta la hipótesis H1 mediante los indicadores empíricos de la VD antes y después de la intervención.
Sintético	Los hallazgos cuantitativos se integran para presentar conclusiones sobre la tendencia observada.

2.2.3 Población y Muestra

La población objetivo corresponde a los usuarios de una organización privada ubicada en la ciudad de Quito (aproximadamente 30 personas del personal administrativo y operativo). La muestra seleccionada corresponde a un grupo piloto de cinco personas, elegidas por conveniencia bajo dos criterios principales: (1) acceso frecuente a correo electrónico corporativo y (2) participación activa en procesos digitales internos.

La selección de escoger cinco participantes sobre los 30 disponibles responde al carácter piloto del estudio: el objetivo es validar el protocolo del programa de intervención y obtener evidencia preliminar sobre la variación en los indicadores de la variable dependiente, más que generar resultados estadísticamente generalizables. Este enfoque es consistente con la naturaleza exploratoria del diseño cuasiexperimental adoptado.

Tabla 4 - Población y muestra del estudio

Elemento	Descripción
Población	Usuarios de la organización en Quito (personal administrativo y operativo)
Tamaño estimado	30 personas
Muestra seleccionada	5 personas (grupo piloto)
Tipo de muestreo	No probabilístico por conveniencia
Grupos involucrados	Personal administrativo (3) y personal operativo con acceso digital (2)

2.2.4 Técnicas e Instrumentos de Recolección de Datos

Tabla 5 - Técnicas e instrumentos de recolección de datos

Técnica	Instrumento	Dimensión VD que mide
Encuesta cuantitativa	Cuestionario digital Likert (15 ítems, escala 1-5) — Google Forms	Perceptual (PEL) — Pre y post intervención
Simulación de phishing	Plataforma GoPhish (código abierto)	Conductual (TCF) y Reactiva (TRC)

2.2.5 Validez y Confiabilidad

La validez se garantiza a través de: validez de contenido (fundamentación en NIST Phish Scale, ISO/IEC 27001, CISA); validez interna (definiciones operacionales claras de los indicadores de la VD); y validez de constructo (alineación entre dimensiones de la VD e instrumentos de medición). El Alfa de Cronbach se presenta como referencia exploratoria de consistencia interna. Con una muestra de cinco participantes ($n = 5$), los valores obtenidos ($\alpha = 0,78$ pretest; $\alpha = 0,82$ posttest) se deben interpretar como evidencia preliminar y no pueden interpretarse como evidencia estadística robusta ya que se recomienda que la muestra sea al menos con 20 participantes ($n \geq 20$) para validaciones más sólidas.

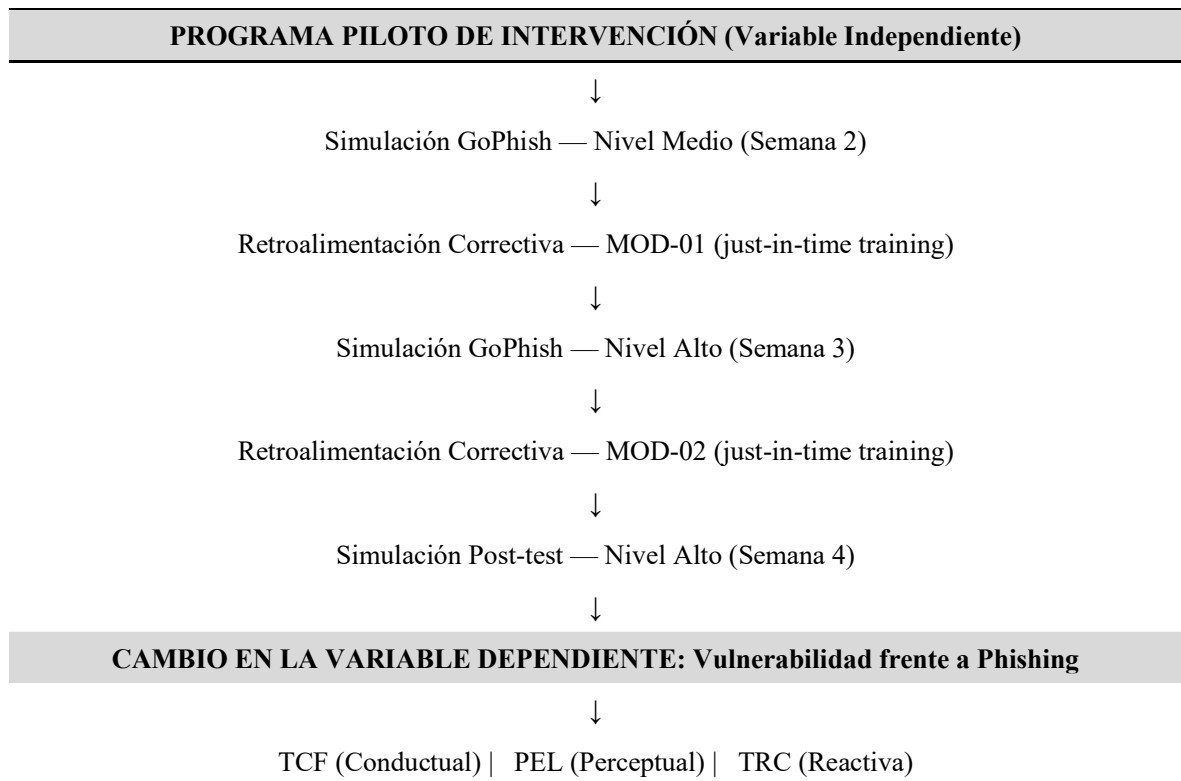
CAPÍTULO III

3. PROPUESTA E IMPLEMENTACIÓN

3.1 DISEÑO DEL PROGRAMA PILOTO

El programa piloto se organiza en cuatro etapas consecutivas distribuidas en cuatro semanas. La Figura 1 presenta el modelo conceptual del programa, que ilustra la secuencia de aplicación de la variable independiente y su efecto esperado sobre la variable dependiente.

Tabla 6 - Modelo conceptual del programa piloto de simulación con retroalimentación correctiva



3.1.1 Etapa 1: Evaluación Inicial (Pre-test) — Semana 1

Se aplica la encuesta Likert de diagnóstico (15 ítems, Google Forms) a los cinco participantes. El instrumento evalúa las tres dimensiones de la VD en su estado inicial. Los

resultados establecen la línea base: PEL pre = 2,40 / 5; TCF Simulación 1 = 80 %; TRC pre = 0 %. El Alfa de Cronbach, como referencia exploratoria de consistencia interna, fue de 0,78.

3.1.2 Etapa 2: Implementación — Simulaciones (Semanas 2-3)

Esta etapa constituye la aplicación de la variable independiente. Durante el programa se realizaron dos simulaciones por participante, calibradas según el NIST Phish Scale:

- Simulación 1 — Nivel Medio (Semana 2): Se envió un correo simulando una alerta bancaria con indicadores de alerta moderados. TCF observada: 80 % (4 de 5 participantes).
- Simulación 2 — Nivel Alto (Semana 3): Se aplicó un ataque de spear phishing incluyendo el nombre real del participante, logotipo corporativo y una firma personalizada. TCF observada: 60 % (3 de 5 participantes).

Inmediatamente tras cada interacción detectada, GoPhish activó de manera automática el módulo de retroalimentación correctiva correspondiente.

3.1.3 Programa de Retroalimentación Correctiva

La retroalimentación correctiva es un componente del programa de intervención (variable independiente), no un objetivo independiente del estudio. Los módulos fueron impartidos inmediatamente después de cada simulación mediante una sesión individual de micro aprendizaje asistida por el investigador, utilizando presentaciones digitales y material audiovisual diseñado específicamente para el estudio. La duración de cada sesión fue de 15

a 20 minutos, con modalidad presencial asistida y acceso complementario en formato digital desde dispositivos móviles o computador.

Tabla 7 - Contenido y características de los módulos de retroalimentación correctiva

Módulo	Tema	Modalidad	Duración	Criterio de aprobación del quiz
MOD-01	Identificación de indicadores de phishing	Presencial asistida + material digital	20 min	$\geq 4 / 5$ respuestas correctas
MOD-02	Verificación de remitentes y análisis de URLs	Presencial asistida + material digital	15 min	$\geq 4 / 5$ respuestas correctas
MOD-03	Procedimientos de reporte de incidentes	Presencial asistida + material digital	15 min	$\geq 4 / 5$ respuestas correctas

Los módulos de retroalimentación fueron desarrollados ad hoc, adaptados al contexto ecuatoriano (servicios bancarios locales, plataformas de gobierno en línea) y alineados con el Control 6.3 de ISO/IEC 27001:2022 y las directrices de CISA. Cada módulo concluye con un quiz de 5 preguntas de opción múltiple. El criterio de aprobación se fijó en 4 o más respuestas correctas ($\geq 80\%$). Los participantes que no alcanzaron este umbral recibieron retroalimentación adicional antes de avanzar con la siguiente fase del programa, asegurando un aprendizaje progresivo.

Recursos utilizados: presentaciones en PowerPoint con capturas de correos reales (anonimizadas), videos cortos que mostraban técnicas de phishing y verificación de URLs, fichas de consulta rápida con indicadores de alerta, y formulario administrado mediante Google Forms para la aplicación del quiz digital.

3.1.4 Etapa 3: Evaluación Final (Post-test) — Semana 4

Se repitió la encuesta Likert y se ejecutó la Simulación 3 (Nivel Alto, escenario de suplantación de licencias de software). Ningún participante hizo clic, registrándose TCF = 0 %. El Alfa de Cronbach post-test, como referencia exploratoria, fue de 0,82.

3.2 CONSIDERACIONES ÉTICAS Y NORMATIVAS

El programa piloto se implementó con estricto apego a principios éticos. Todos los participantes firmaron consentimiento informado antes del inicio. Se garantizó la confidencialidad y los resultados se presentan de forma agregada. La plataforma GoPhish fue configurada en servidor local para evitar el procesamiento de datos por terceros. El proyecto cumple con los principios de finalidad, proporcionalidad y seguridad de la LOPDP (Ecuador, 2021) y las recomendaciones de ASIS International sobre prácticas éticas en simulaciones de phishing.

CAPÍTULO IV

4. RESULTADOS Y ANÁLISIS

4.1 RESULTADOS POR PARTICIPANTE

A continuación, se presentan los resultados obtenidos en las tres fases del diseño cuasiexperimental. Los insumos completos (respuestas individuales por ítem y registros de GoPhish) se encuentran en los Anexos.

Tabla 8 - Resultados por participante — Variable dependiente (dimensiones conductual, perceptual y reactiva)

Part.	TCF Sim.1 (Pre)	TCF Sim.2	TCF Sim.3 (Post)	PEL Pre	PEL Post	Δ PEL	TRC Post
P1	1 (Clic)	1 (Clic)	0 (No)	2,3	3,9	+70 %	Sí
P2	1 (Clic)	0 (No)	0 (No)	2,1	3,7	+76 %	Sí
P3	1 (Clic)	1 (Clic)	0 (No)	2,6	3,8	+46 %	No
P4	0 (No)	0 (No)	0 (No)	2,5	3,8	+52 %	Sí
P5	1 (Clic)	1 (Clic)	0 (No)	2,5	3,8	+52 %	No
TOTAL	80 %	60 %	0 %	2,40 / 5	3,80 / 5	+58 %	60 %

4.2 VARIACIÓN DE LOS INDICADORES DE LA VARIABLE DEPENDIENTE

Tabla 9 - Comparación de indicadores VD (Pre vs. Post intervención)

Dimensión VD	Indicador		Pre	Post	Variación observada
Conductual	Tasa de Clics (TCF)		80 %	0 %	Reducción observada del 100 % (meta: < 30 %) — Tendencia favorable
Perceptual	Puntaje (PEL)	Likert	2,40 / 5	3,80 / 5	Incremento observado del 58 % (meta: ≥ +0,8 pts) — Tendencia favorable
Reactiva	Tasa de Reporte (TRC)		0 %	60 %	Incremento observado (meta: ≥ 60 %) — Meta alcanzada

Dimensión VD	Indicador	Pre	Post	Variación observada
Consistencia	Alfa de Cronbach (ref. exploratoria)	0,78	0,82	Superó umbral de 0,70 en ambas mediciones

4.3 ANÁLISIS DE LOS RESULTADOS

La tasa de clics en enlaces fraudulentos (TCF) registró una reducción observada de 80 % a 0 %, superando la meta establecida. Esta tendencia favorable es consistente con los rangos documentados en estudios similares (Timko et al., 2024), sin embargo, es importante señalar que, debido al tamaño reducido de la muestra ($n = 5$) y la ausencia de grupo control, no es posible establecer una causalidad fuerte ni generalizar los hallazgos.

Los resultados responden a un grupo piloto reducido y altamente supervisados, por lo que es posible que podrían no reproducirse con la misma magnitud en poblaciones más amplias o en contextos con menor grado de control.

La puntuación Likert promedio registró un incremento observado de 2,40 a 3,80 puntos (+58 %). La tasa de reporte de correos sospechosos pasó de 0 % a 60 %, alcanzando la meta propuesta. El Alfa de Cronbach, presentado como referencia exploratoria de consistencia interna, fue de 0,78 (pretest) y 0,82 (postest), superando el umbral de 0,70 recomendado para estudios exploratorios.

En conjunto, los tres indicadores muestran una tendencia favorable en la variable dependiente tras la aplicación del programa de intervención. Estos resultados constituyen evidencia preliminar que sugiere que la intervención contribuyó a reducir la vulnerabilidad observada en los participantes, en línea con la hipótesis H1.

4.4 HALLAZGOS COMPLEMENTARIOS

Como complemento al análisis cuantitativo, se recogieron percepciones de los participantes mediante entrevistas breves realizadas en la fase post-test. Los hallazgos más relevantes se resumen a continuación:

En cuanto al realismo de las simulaciones, la mayoría de los participantes señaló que los correos simulados —especialmente el de nivel alto (spear phishing personalizado)— fueron difíciles de distinguir de comunicaciones legítimas. Un participante indicó: "No lo dudé porque usaba mi nombre y el logo de la empresa". Este tipo de respuestas confirma la pertinencia del diseño de los escenarios y la validez del NIST Phish Scale como herramienta de calibración ya que consigue recrear condiciones realistas que ponen a prueba la capacidad de detección de los usuarios.

En cuanto a la utilidad de la retroalimentación correctiva, los participantes destacaron que la sesión inmediata al error resultó el elemento más valorado de la intervención. Un participante señaló que "verlo en el momento en que me equivoqué fue mucho más efectivo que cualquier charla teórica". Esto es coherente con la evidencia de la literatura sobre el just-in-time training (León Naranjo et al., 2025).

En relación al cambio conductual percibido, todos los participantes reportaron mayor cautela al revisar correos electrónicos corporativos tras la intervención. Tres de ellos indicaron que ahora verifican el remitente y la URL antes de hacer clic en cualquier enlace, lo que sugiere un cambio en la dimensión conductual de la VD que va más allá de lo medido por la TCF en la Simulación 3.

4.5 COHERENCIA ENTRE OBJETIVOS, METODOLOGÍA Y RESULTADOS

Tabla 10 - Mapa de coherencia interna del estudio

Componente	Contenido
Objetivo general	Evaluar la efectividad del programa de intervención (VI) sobre la Variable dependiente.
Hipótesis H1	El programa se asocia con una reducción en la vulnerabilidad (evidencia preliminar).
Diseño	Cuasi-experimental $O1 \rightarrow X \rightarrow O2$, enfoque predominantemente cuantitativo.
VI	Programa de simulación de phishing con retroalimentación correctiva.
VD (3 dim.)	TCF (conductual) + PEL (perceptual) + TRC (reactiva).
Resultados	Se observó tendencia favorable en los tres indicadores dentro del grupo piloto controlado.
Conclusión	Los resultados sugieren que la intervención contribuyó a reducir la vulnerabilidad observada.

4.6 ALINEACIÓN CON ESTÁNDARES INTERNACIONALES

Tabla 11 - Cumplimiento de estándares internacionales

Estándar	Requerimiento	Evidencia	Estado
ISO/IEC 27001:2022 — Control 6.3	Concienciación, educación y formación en seguridad.	Módulos de retroalimentación correctiva + encuesta Likert.	Cumplido
NIST Phish Scale (NIST TN 2276)	Simulaciones calibradas por nivel de dificultad.	Sim. 1 (Nivel Medio) + Sim. 2 (Nivel Alto).	Cumplido
CISA Phishing Guidance (2023)	Retroalimentación basada en simulaciones.	Retroalimentación correctiva inmediata post-simulación.	Cumplido
LOPDP — Decreto 904/2023	Consentimiento informado y confidencialidad.	Formulario de consentimiento firmado por cada participante.	Cumplido

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. Los resultados obtenidos sugieren que el programa piloto de simulación de phishing con retroalimentación correctiva contribuyó a reducir la vulnerabilidad observada en los participantes frente a ataques de ingeniería social, evidenciada por una tendencia favorable en las tres dimensiones de la variable dependiente: conductual (TCF de 80 % a 0 %), perceptual (PEL de 2,40 a 3,80, +58 %) y reactiva (TRC de 0 % a 60 %). Dado que los resultados responden a un grupo piloto reducido y altamente controlado, no necesariamente se reproducirán con igual magnitud en poblaciones mayores. Los hallazgos constituyen evidencia preliminar y no permiten afirmar causalidad fuerte dada la ausencia de grupo control.
2. El diseño cuasi-experimental de pre-test y post-test con un solo grupo proporcionó una estructura metodológica coherente para identificar la variación en los indicadores de la VD antes y después de la intervención, coherente con el objetivo general de evaluar la efectividad del programa. La lógica interna del estudio —desde el diagnóstico hasta las conclusiones— se mantuvo consistente en todas sus secciones.
3. El contexto ecuatoriano —caracterizado por el rápido crecimiento del comercio electrónico (más de 81 millones de transacciones en 2024) y el incremento de los ataques de phishing (12,2 millones de ataques bloqueados en 2023)— confirma la pertinencia de iniciativas como la propuesta. Además, la alineación con la LOPDP e ISO/IEC 27001:2022 garantiza su validez normativa.

4. El uso de herramientas de código abierto (GoPhish) y materiales adaptados al contexto ecuatoriano redujo las barreras económicas, lo que hace viable el programa para organizaciones medianas y pequeñas. Este factor de accesibilidad es clave para su escalamiento en el sector privado ecuatoriano.

5. El factor humano se confirmó como el eslabón más vulnerable dentro de la cadena de seguridad. La retroalimentación correctiva experiencial (just-in-time training) mostró, en este estudio piloto, una tendencia favorable para modificar comportamientos de riesgo, en línea con el Control 6.3 de ISO/IEC 27001:2022 y con los hallazgos reportados en la literatura especializada.

5.2 RECOMENDACIONES

1. Escalar el programa piloto a muestras más amplias —mínimo 20 a 30 participantes— que permitan obtener resultados estadísticamente defendibles y generalizar las conclusiones. Se recomienda incorporar un grupo control para fortalecer la validez interna y permitir afirmaciones causales más robustas.

2. Implementar programas de simulación de forma continua y periódica (mínimo dos veces al año), dado que la evidencia muestra que los efectos de las intervenciones de este tipo decaen en el tiempo si no se refuerzan regularmente, con actualizaciones sobre nuevas tipologías de phishing potenciadas por inteligencia artificial generativa.

3. Las organizaciones ecuatorianas deberían integrar los programas de simulación dentro de sus Sistemas de Gestión de Seguridad de la Información (SGSI) formales, esto no solo responde al cumplimiento del Control 6.3 de ISO/IEC 27001:2022 sino que también

permite documentar métricas de efectividad y demostrar cumplimiento normativo frente auditorías.

4. Promover desde el Gobierno ecuatoriano la adopción de programas de concienciación en ciberseguridad como requisito para las organizaciones que manejan datos personales, en el marco de la LOPDP, con incentivos regulatorios que aceleren su adopción en el sector privado.

5. Para futuras investigaciones, explorar la efectividad de técnicas de gamificación y simulaciones multicanal (phishing por SMS, redes sociales y llamadas telefónicas), incorporar análisis de seguimiento longitudinal para medir la retención de los efectos de la intervención, y ampliar la muestra para validar estadísticamente los hallazgos preliminares del presente estudio.

REFERENCIAS

- Barrera, D., Naranjo, V., Fuertes, W., & Macas, M. (2024). Literature review of SMS phishing attacks. En T. Guarda et al. (Eds.), ARTIIS 2023 (CCIS 1936) (pp. 191–204). Springer. https://doi.org/10.1007/978-3-031-48855-9_15
- CECE & UEES. (2025). Estudio Ecommerce 2025: VII Medición. <https://cece.ec/wp-content/uploads/estudios-ecommerce-ec/Estudio-Ecommerce2025-VII-Medicion.pdf>
- CISA/NSA/FBI/MS-ISAC. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One. <https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>
- Dawkins, S., & Jacobs, J. (2023). NIST Phish Scale User Guide (NIST TN 2276). NIST. <https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2276.pdf>
- Deloitte Ecuador. (2023). Estado Actual de la Ciberseguridad Ecuador 2023. <https://www.deloitte.com/latam>
- Elsadig, M., Ibrahim, A. O., Basheer, S., et al. (2022). Intelligent deep ML cyber phishing URL detection based on BERT features extraction. *Electronics*, 11(22), 3647. <https://doi.org/10.3390/electronics11223647>
- Herrera Ruiz, S. (2024). Informe e-País: El comercio electrónico en Ecuador. ICEX.
- IBM. (2024). Cost of a Data Breach Report 2024. <https://www.ibm.com/reports/data-breach>

- ITAhora. (2024). Amenazas en Ecuador: malware, phishing y el rol de la inteligencia de amenazas. <https://itahora.com/2024/09/03/amenazas-en-ecuador-malware-phishing-y-el-rol-de-la-inteligencia-de-amenazas/>
- Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing detection system through hybrid machine learning based on URL. *IEEE Access*, 11, 24728–24742. <https://doi.org/10.1109/ACCESS.2023.3245820>
- Kaspersky LATAM. (2023). Nueva epidemia: el phishing se sextuplicó en América Latina. <https://latam.kaspersky.com/about/press-releases/nueva-epidemia-el-phishing-se-sextuplico-en-america-latina>
- León Naranjo, J. R., Oleas Morán, M. M., & Pimentel Salazar, K. Z. (2025). El papel de la inteligencia artificial en la detección del phishing. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, 6(4). <https://doi.org/10.56712/latam.v6i4.4437>
- Martí Ramírez, T. (2025). Evolution of Phishing Cyberattacks Using Artificial Intelligence. *ULACIT*.
- Meléndez, R., Ptaszynski, M., & Masui, F. (2024). Comparative investigation of traditional ML and transformer models for phishing email detection. *Electronics*, 13(24), 4877. <https://doi.org/10.3390/electronics13244877>
- Microsoft. (2025). Fraude basado en IA: Nuevas amenazas y estrategias de mitigación. <https://news.microsoft.com/es-es/2025/04/16/fraude-basado-en-ia-nuevas-amenazas-y-estrategias-de-mitigacion/>

- Paucar Cordova, J. A. (2025). Phishing in the Digital Era: A Systematic Review of the Most Promising Detection Techniques. LACCEI 2025.
- PCG. (2025). ISO 27001:2022 – All Changes & 11 New Controls Explained. <https://pcg.io/insights/iso-27001-2022-new-controls/>
- PECB. (2022). ISO/IEC 27001 – What are the main changes in 2022?. <https://pecb.com/en/article/iso-iec-27001-what-are-the-main-changes-in-2022>
- Presidencia de la República del Ecuador. (2023). Reglamento General de la LOPDP (Decreto 904).
- Primicias. (2023). Ecuador encabeza el listado de países con más ataques de phishing. <https://www.primicias.ec/noticias/tecnologia/ecuador-deteccion-ataques-phishing/>
- PT Security. (2025). Cybersecurity threatscape for Latin America and the Caribbean: 2023–2024.
- República del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales (R.O. 459).
- SOCRadar. (2024). LATAM Threat Landscape Report 2024.
- Somesha, M., & Pais, A. R. (2022). Classification of phishing email using word embedding and ML techniques. *Mobility*, 11(3), 279–320.
- Timko, D., Hernandez Castillo, D., & Rahman, M. L. (2024). A quantitative study of SMS phishing detection. arXiv. <https://arxiv.org/abs/2311.06911>
- Verizon. (2024). Data Breach Investigations Report 2024. <https://www.verizon.com/business/resources/reports/dbir/>

ANEXOS

Anexo 1: Encuesta de Diagnóstico — Variable Dependiente Dimensión Perceptual (Pre-test y Post-test)

Instrucciones: Responda las siguientes preguntas usando la escala: 1 = Totalmente en desacuerdo / Nunca, 2 = En desacuerdo / Casi nunca, 3 = Neutral / A veces, 4 = De acuerdo / Frecuentemente, 5 = Totalmente de acuerdo / Siempre.

Dimensión 1: Conocimiento sobre phishing

1. Sé identificar qué es un ataque de phishing por correo electrónico.
2. Puedo distinguir las características de un correo electrónico legítimo de uno fraudulento.
3. Conozco las principales técnicas que utilizan los atacantes en correos de phishing.
4. Sé qué acciones debo tomar si recibo un correo electrónico sospechoso.
5. Estoy familiarizado/a con las políticas de seguridad de la información de mi organización.

Dimensión 2: Percepción de riesgo

6. Considero que mi organización es un blanco potencial de ataques de phishing.
7. Creo que podría ser víctima de un ataque de phishing en mi trabajo.
8. Considero que las consecuencias de un ataque de phishing exitoso serían graves para mi organización.

9. Percibo que el nivel de amenaza de phishing ha aumentado en los últimos años.
10. Creo que la protección técnica (antivirus, filtros de correo) es suficiente para protegerme del phishing.

Dimensión 3: Comportamientos de seguridad

11. Verifico el remitente antes de abrir un correo electrónico inesperado.
12. Evito hacer clic en enlaces de correos electrónicos que no esperaba recibir.
13. Reporto correos sospechosos al equipo de tecnología de mi organización.
14. Utilizo contraseñas diferentes para distintos servicios digitales.
15. He participado en capacitaciones de seguridad de la información en los últimos 12 meses.

Anexo 2: Guía de Entrevista (Post-test — Complemento cualitativo)

16. ¿Cómo describiría su experiencia al recibir los correos simulados de phishing? ¿Qué sintió en ese momento?
17. ¿Cuáles fueron las características del correo que lo llevaron a hacer clic (o a no hacerlo)?
18. ¿Qué aspectos de la retroalimentación correctiva considera más útiles para su trabajo diario?

19. ¿Cómo ha cambiado su comportamiento al revisar correos electrónicos después de la intervención?

20. ¿Qué recomendaría para mejorar el programa de simulación?

Anexo 3: Cronograma de Implementación del Programa Piloto

Tabla 12 - Cronograma del programa piloto

Semana	Actividad	Componente del Diseño	Responsable
Semana 1	Encuesta pre-test + Línea base VD	Medición VD — Pre-test	Investigador Participantes /
Semana 2	Simulación 1 (Nivel Medio) + Retroalimentación MOD-01	Aplicación VI — Fase 1	Investigador
Semana 3	Simulación 2 (Nivel Alto) + Retroalimentación MOD-02	Aplicación VI — Fase 2	Investigador
Semana 4	Simulación post-test + Encuesta post-test + Análisis VD	Medición VD — Post-test	Investigador