
**UNIVERSIDAD NACIONAL DE CHIMBORAZO**
**FACULTAD DE INGENIERÍA**
**CARRERA INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN**

# Técnicas de ingeniería social y estrategias de mitigación para la protección de datos personales y corporativos en sistemas de correo empresariales

**Trabajo de Titulación para optar al título de**
**Ingeniero en Tecnologías de la Información**

**Autores:**
**Cabezas Arce, Jandry Alexander**
**Chacón Goyes, Alain Josue**

**Tutor:**
**Ing. Danny Patricio Velasco Silva Mgs.**

**Riobamba, Ecuador. 2026**

# DECLARATORIA DE AUTORÍA

Nosotros, Jandry Alexander Cabezas Arce, con cédula de ciudadanía 2200553812, y Alain Josue Chacón Goyes, con cédula de ciudadanía 0605147271, autores del trabajo de investigación titulado: Técnicas de ingeniería social y estrategias de mitigación para la protección de datos personales y corporativos en sistemas de correo empresariales, certificamos que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de nuestra exclusiva responsabilidad.

Asimismo, cedemos a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor(es) de la obra referida será de nuestra entera responsabilidad, librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 14 de mayo del 2026.

Jandry Alexander Cabezas Arce
C.I: 2200553812

Alain Josue Chacón Goyes
C.I: 0605147271

# DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Danny Patricio Velasco Silva, catedrático adscrito a la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: TÉCNICAS DE INGENIERÍA SOCIAL Y ESTRATEGIAS DE MITIGACIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES Y CORPORATIVOS EN SISTEMAS DE CORREO EMPRESARIALES, bajo la autoría de Jandry Alexander Cabezas Arce y Alain Josue Chacón Goyes; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 14 días del mes de mayo de 2026

Danny Patricio Velasco Silva
C.I: 0602768640

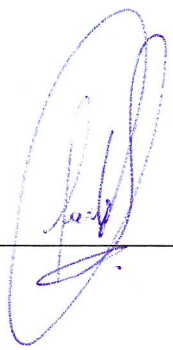
# CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación "TÉCNICAS DE INGENIERÍA SOCIAL Y ESTRATEGIAS DE MITIGACIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES Y CORPORATIVOS EN SISTEMAS DE CORREO EMPRESARIALES", presentado por Jandry Alexander Cabezas Arce, con cédula de identidad 2200553812, y Alain Josue Chacón Goyes, con cédula de identidad 0605147271, bajo la tutoría del Mgs. Danny Patricio Velasco Silva; certificamos que recomendamos la APROBACIÓN del mismo con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de sus autores, no teniendo más nada que observar.

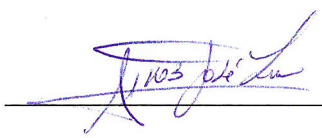
De conformidad a la normativa aplicable firmamos, en Riobamba 30 de junio del 2026

Ing. Fernando Molina
**PRESIDENTE DEL TRIBUNAL DE GRADO**

Ing. Lady Espinoza
**MIEMBRO DEL TRIBUNAL DE GRADO**



Ing. José Jinez
**MIEMBRO DEL TRIBUNAL DE GRADO**



# CERTIFICACIÓN

Que, **CABEZAS ARCE JANDRY ALEXANDER** con CC: **2200553812** y **CHACÓN GOYES ALAIN JOSUE** con CC: **0605147271**, estudiantes de la Carrera **INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN**, Facultad de **INGENIERÍA**; han trabajado bajo mi tutoría el trabajo de investigación titulado **"TÉCNICAS DE INGENIERÍA SOCIAL Y ESTRATEGIAS DE MITIGACIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES Y CORPORATIVOS EN SISTEMAS DE CORREO EMPRESARIALES"**, cumple con el 10 %, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 15 de mayo de 2026

DANNY PATRICIO VELASCO SILVA

Ing. Danny Patricio Velasco Silva
**TUTOR**

# DEDICATORIA

Dedico mi tesis a toda mi familia, principalmente a mi mamá Maira Alejandra Arce Vera que ha sido la persona que me ha apoyado en todo este camino de altas y bajas, que ha conocido mis miedos y me ha dado la fuerza para seguir cada día, con la esperanza de darle todo el mundo. A mis hermanos y mi primo, que también han sido una luz para seguir adelante y tratando de ser un ejemplo para ellos, esperando que tengan un futuro mucho más brillante.
Dedico también esta tesis a todos mis amigos, los que han estado ahí desde el primer día que empecé esta carrera, y han sido un apoyo incondicional cuando creí que ya no podía más. A esos profesionales dentro de la carrera que lograron darme el apoyo necesario para dar de mi potencial.
Por último, quiero dedicar esta tesis a mi gata Kiki que ha sido mi compañera en trasnochadas y en tantos malos momentos, así como también muy buenos momentos.

***Jandry Alexander Cabezas Arce***

Dedico mi tesis a mis padres, tanto de sangre como de afinidad, que con su incondicional apoyo hicieron posible que pueda conseguir mi sueño de estudiar la carrera que me apasiona. A mis abuelitos, que con su experiencia y consejos en el viaje de la vida me dieron guía para poder seguir en el camino del bien. A mis hermanos, a los que espero servir de ejemplo para que cuando se encuentren con la adversidad de la vida tengan un referente, y a los que espero tengan un camino muchísimo más brillante que el mío.
Dedico también esta tesis a los profesionales que hicieron posible que llegue a donde estoy ahora. A mis profesores y docentes, que con su abanico de conocimiento en la materia labraron mis saberes y mi carácter con disciplina para volverme un profesional de bien. Y a

aquellos profesionales en su campo, que durante los momentos de adversidad me lograron dar el apoyo necesario para afrontar la adversidad y frustración que traen los altibajos de la vida.
Finalmente, dedico esta tesis a mis compañeros que estuvieron junto a mí en la batalla por volverme profesional. Y, sobre todo, a todas aquellas personas que tengo el honor de llamar amigos, a aquellos que siguen a mi lado en el transcurso de esta etapa, aquellos que viajaron en búsqueda de cumplir sus sueños y que la distancia no ha hecho más que fortalecer esta unidad, y aquellos que ya no están entre nosotros cuyo recuerdo vivirá por siempre en mi memoria y planeo honrar viviendo una vida plena cumpliendo todo lo que en vida les prometí llegar a ser.

***Alain Josue Chacón Goyes***

# AGRADECIMIENTO

Quiero agradecer a mis familiares que siempre han creído en mí y en todo lo que soy capaz de lograr, agradecer por hacerme dado su apoyo y nunca dejar de creer en mí, brindándome motivación para seguir adelante frente a la adversidad.
Me gustaría agradecer a mi tutor de tesis por darnos guía en todo este proceso caótico.
También me gustaría agradecer a los docentes que tuve durante todo mi proceso de formación profesional.
Y por último me gustaría agradecer a las personas que ya no están a mi lado, pero dejaron una huella imborrable en mi camino. Gracias a todos ellos por ayudarme a ser la persona que seré.

***Jandry Alexander Cabezas Arce***

Agradezco a mis familiares, por haberme brindado su apoyo y consejo durante todo el tramo de este viaje que fue la universidad habiéndome dado motivación y guía en los momentos donde más me sentía perdido.
De igual forma, extiendo mi especial agradecimiento a nuestro tutor de tesis que nos brindó guía durante el último trayecto del viaje para volvernos profesionales. Su asesoría nos fue crucial a la hora de elaborar este trabajo que sin ella no hubiéramos podido realizar este trabajo.
Así mismo, agradezco a los docentes y tutores que me enseñaron los conocimientos necesarios para mi tramo como profesional. Finalmente, agradezco a mis amigos y compañeros que me acompañaron en el trayecto de formación.

***Alain Josue Chacón Goyes***

# ÍNDICE GENERAL

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# RESUMEN

El aumento en los ataques de ingeniería social en el Ecuador representa un desafío para las distintas instituciones que utilizan herramientas tecnológicas en su infraestructura ya que los ataques de ingeniería social están dirigidos al componente humano en lugar de los sistemas. Mediante revisión de literatura y un levantamiento de información técnica al sistema de correos basada en entrevistas al personal a cargo del sistema de correo electrónico y cuestionarios piloto aplicados a usuarios con perfiles con y sin conocimiento técnico en tecnología se elaboraron estrategias de mitigación y políticas de seguridad para la protección de datos personales; a partir de las estrategias y políticas desarrolladas, se elaboró un programa de capacitación para el cuerpo universitario; y para evaluar la efectividad de dichas políticas y estrategias, se desarrolló un cuasiexperimento con Pretest y Postest y grupo de control donde se evaluó el impacto de la capacitación creada a partir de las políticas y estrategias sobre una muestra de 30 sujetos divididos en dos grupos de 15 pertenecientes a la facultad de Ciencias Políticas y Administrativas de la UNACH a partir de la función Detectar del marco de ciberseguridad NIST. La evaluación de la efectividad de las políticas y estrategias aplicadas a través del programa mediante la prueba de McNemar indicó que estas fueron parcialmente efectivas a la hora de proteger datos ya que se detectó un aumento en la cantidad de reportes de correos maliciosos ($p=0.0026$), pero no se consiguió reducir los comportamientos como apertura de los correos ($p=0.61$), clic en enlaces maliciosos ($p=0.07$) y divulgación de datos personales ($p=1.00$).

**Palabras claves**: Ingeniería social, correo electrónico, phishing, mitigación de riesgos, políticas de seguridad, NIST CSF, protección de datos.

# ABSTRACT

The increase in social engineering attacks in Ecuador poses a critical challenge for institutions relying on digital infrastructure, as these threats exploit human vulnerabilities rather than system flaws. This study developed data protection policies and mitigation strategies for a university email system, utilizing a literature review and technical information gathered through staff interviews and user pilot questionnaires. These strategies were subsequently integrated into a comprehensive training program for the university body. To evaluate the training's effectiveness, a quasi-experimental design was implemented featuring a pre-test, post-test, and control group. The sample comprised 30 subjects from the Faculty of Political and Administrative Sciences at UNACH, split into two equal groups of 15, with evaluation metrics aligned to the Detect function of the NIST cybersecurity framework. Statistical analysis using McNemar's Test indicated that the intervention was only partially effective. While the training significantly increased the reporting of malicious emails ($p=0.0026$), it failed to yield statistically significant reductions in risky behaviors, including opening suspicious emails ($p=0.61$), clicking on malicious links ($p=0.07$), and disclosing personal data ($p=1.00$).



**Key words**: Social engineering, Cybersecurity training, NIST framework, Quasi-experiment, Ecuador.


Reviewed and improved by Jacqueline Armijos

# CAPÍTULO I. INTRODUCCIÓN

En la era de la transformación digital, los datos personales y corporativos constituyen un activo estratégico para las organizaciones, cuya protección es esencial para garantizar su continuidad operativa y reputación. Los sistemas de correo electrónico empresariales, como los utilizados por la Universidad Nacional de Chimborazo (UNACH), son un punto crítico de vulnerabilidad frente a amenazas cibernéticas, especialmente aquellas basadas en técnicas de ingeniería social. Estas técnicas, definidas como métodos de manipulación psicológica para obtener acceso no autorizado a información o sistemas [1], explotan el factor humano, Respaldado por la evidencia empírica reciente, según la cual el elemento humano estuvo presente en el 68% de las brechas de seguridad confirmadas a nivel global [2].

El incremento de ataques de ingeniería social en Ecuador representa un desafío para todas las instituciones que utilizan herramientas tecnológicas en su infraestructura; dentro de estas instituciones se encuentran universidades como la UNACH que gestiona la información a través de los sistemas de Microsoft 365. Pero el problema no es el software, sino cómo los usuarios se protegen ante la amenaza de la ingeniería social porque no poseen el conocimiento para cuidarse y la universidad no tiene políticas que promuevan una cultura de protección ante ingeniería social. Los usuarios universitarios son responsables de proteger su información sensible, tienen que adoptar buenas prácticas. Pero sin programas de capacitación en ciberseguridad y sin políticas claras para frenar los riesgos, la institución no puede esperar que los usuarios hagan todo el trabajo solos ya que no poseen las herramientas.

El NIST Cybersecurity Framework es un marco voluntario para gestionar y reducir el riesgo de ciberseguridad, creado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés National Institute of Standards and Technology) que busca ayudar a las organizaciones, especialmente a las que poseen una infraestructura crítica. En Ecuador, la Ley orgánica de protección de datos personales exige que instituciones como la UNACH protejan datos sensibles con medidas preventivas. NIST CSF ofrece un camino: capacitar usuarios, evaluar riesgos, establecer políticas. Todo esto funciona dentro del marco que ya se tiene.

Este trabajo de titulación analiza las principales técnicas de ingeniería social y desarrolla estrategias de mitigación específicas para el correo de la UNACH que incluyen políticas de seguridad y estrategias basadas en el NIST CSF que buscan fortalecer la protección de datos personales y corporativos sin requerir cambios en Microsoft 365.

## 1.1 Planteamiento del problema

La transformación digital ha posicionado a los sistemas de correo electrónico como una herramienta esencial para la comunicación y gestión de datos en entornos empresariales y académicos. Pero este salto incrementó la exposición a amenazas cibernéticas ingeniería social basadas en el factor humano como eslabón más débil en la estructura de los sistemas informáticos de las organizaciones. La UNACH hace uso de Microsoft 365 para el correo institucional con el cuál maneja datos sensibles e información sobre el entorno administrativo de la universidad. El sistema es robusto, pero los atacantes también lo saben. El phishing, el

pretexting y el spoofing funcionan aquí como en cualquier otro lugar. Estos tres métodos representan casi el 75% de brechas de seguridad a nivel global [2].

En Ecuador, los ataques de ciberseguridad están aumentando. El phishing es el riesgo más inmediato. En la UNACH, estudiantes, administrativos y docentes están expuestos porque no hay capacitación formal ni políticas diseñadas para defenderse. Un phishing exitoso roba credenciales y los atacantes hacen uso de estas mismas para tener acceso a todo: robo de datos, robo de identidad, ataques dirigidos, etc. La política de protección de datos personales de la UNACH de 2020 establece normas para credenciales, pero no aborda la ingeniería social y esto reduce su efectividad [3].

Un levantamiento de información técnica confirmó la sospecha de que la UNACH depende de la configuración predeterminada de Microsoft 365. Tiene un nivel de protección básico, pero crea un problema al dejar vulnerabilidades abiertas y la institución reacciona después de que los atacantes ya se infiltraron dentro del sistema. Hay un segundo problema más claro todavía. En 2025, los administrativos recibieron capacitación obligatoria en ciberseguridad. Los estudiantes no. Eso es una brecha porque los estudiantes son quienes más tráfico generan en la red, siendo el eslabón débil. Añadido a eso, la falta de simulaciones de phishing periódicas y la nula difusión para el uso de canales de denuncia como el canal "mesadeayuda@unach.edu.ec" crean un punto ciego en la arquitectura de defensa y seguridad de la institución.

Esta investigación aborda estas deficiencias pasando de la observación pasiva a la intervención activa y aplicada.

## 1.2 Justificación

Dentro de un entorno empresarial, los datos conforman el activo digital más valioso de la institución; Sin embargo, los sistemas de seguridad se limitan al factor humano y a cómo cada usuario responde ante una amenaza que no ataca directamente al sistema sino a los propios usuarios. Toda institución necesita protegerse ante este tipo de amenazas ya que un firewall no es suficiente cuando el ataque utiliza palabras para despistar al personal y provocar una acción maliciosa. Se necesita establecer políticas de protección y capacitar a los usuarios para que se cree una cultura en donde se dude antes de actuar.

Este trabajo desarrolla estrategias y políticas específicas para la UNACH, enfocadas en proteger a los usuarios contra estos ataques, buscando crear una cultura de seguridad.

## 1.3 Formulación del problema

¿Cómo influyen las técnicas de ingeniería social y estrategias de mitigación en la efectividad de la protección de datos personales y corporativos en sistemas de correo empresariales?

## 1.4 Objetivos

## Objetivo general

Analizar las técnicas de ingeniería social y desarrollar estrategias de mitigación basadas en formación y políticas de seguridad para proteger los datos personales y corporativos en los sistemas de correo electrónico institucional de la Universidad Nacional de Chimborazo, considerando elementos del núcleo del Marco de Seguridad NIST (NIST CSF)

## Objetivos específicos

- Identificar y analizar las principales técnicas de ingeniería social que amenazan la seguridad de los datos en los sistemas de correo electrónico institucional de la UNACH, mediante revisión de literatura y análisis de casos locales.

- Diseñar e implementar estrategias de mitigación no invasivas, como programas de formación en ciberseguridad y políticas de seguridad, para fortalecer la protección de datos en los sistemas de correo electrónico de la UNACH, sin modificar la infraestructura de Microsoft 365.

- Evaluar la efectividad de la protección de datos personales y corporativos aplicando las técnicas de ingeniería social y estrategias de mitigación, utilizando el Marco de Seguridad NIST (NIST CSF).

# CAPÍTULO II. MARCO TEÓRICO

Para el trabajo de titulación, es importante que se analicen las técnicas de ingeniería social de manera general, ya que su estructuración sirve como punto de apoyo para elaborar políticas y estrategias que permitan proteger ante dichas amenazas; del mismo modo, un levantamiento de información técnica realizado al sistema de correo institucional permite relacionar hallazgos del primer análisis con la realidad de la institución para encontrar los puntos débiles que se deban proteger en las políticas y estrategias.

## 2.1 Estado del arte

Entre los estudios revisados que entran en la materia de estudio del trabajo, se encontraron hallazgos como los del trabajo de Althobaiti y Alsufyani [4], que tras una revisión literaria concluyeron que el phishing es una amenaza de gran vigor para la ciberseguridad de las organizaciones del mundo; además, encontraron que la literatura actual se centra en la detección y concientización sobre el phishing, pero que es necesario profundizar en el desarrollo de estrategias de prevención y mitigación señalando la necesidad de desarrollar técnicas eficaces que cubran estas carencias en los modelos actuales de protección.

Otros trabajos como el realizado por Brooks y McAndrew [5], donde se realizó un análisis cualitativo a expertos de TI sobre su experiencia manejando los programas de concientización en ciberseguridad en sus respectivas empresas, señalan la importancia para mitigar los ataques de ingeniería social de las simulaciones de phishing, la autenticación doble factor (MFA) y el entrenamiento basado en escenarios reales, el estudio encontró que los programas basados en concientización mejoraron la protección en sus empresas.

Otros hallazgos como los del trabajo de Morić et al. [6], donde se realizaron simulaciones de phishing en una cronología distinta, encontró un alto riesgo de compromiso de información en períodos donde la carga de trabajo crece, como antes de un feriado; así mismo, el trabajo de Alhaddad et al. [7], que, tras realizar una simulación de phishing sobre una muestra donde se conocía su perfil de personalidad, encontró que el programa de capacitación instantáneo redujo positivamente la cantidad de clics de los usuarios en correos maliciosos.

Tras la revisión de los trabajos de otros investigadores, se puede concluir lo siguiente: Hay una necesidad global en el desarrollo de estrategias de nuevas técnicas de protección ante la ingeniería social; y también que, las simulaciones de phishing y el entrenamiento basado en escenarios reales es efectivo para mejorar la seguridad y la preparación de los usuarios ante la amenaza de la ingeniería social, esta última se puede valer de programas de capacitación al momento que demostraron ser efectivos para lograr este cometido.

## 2.2 La ingeniería social como amenaza a la ciberseguridad

La ingeniería social consiste en la manipulación de las personas para que revelen datos confidenciales o garanticen acceso a sistemas críticos aprovechando el factor psicológico en lugar de atacar directamente al sistema informático [8]. Dentro del marco de la ciberseguridad, un sistema informático lo conforma el componente informático y el componente humano; se considera a este último como el eslabón más débil de este sistema [9], ya que como menciona

Kevin Mitnick, uno de los hackers más famosos por su empleo de técnicas de ingeniería social, los humanos son susceptibles al engaño debido a las tendencias de su psiquis a la complacencia y la obediencia [10], en la tabla 1 se muestran las tendencias humanas consideradas aprovechables por los ingenieros sociales que Mitnick resume en su libro a partir del trabajo de Robert B. Cialdini en la revista Scientific American.

**Tabla 1:** Tendencias básicas del comportamiento humano.

| Tendencia | Causa de complacencia |
|---|---|
| Autoridad | Los humanos tienden a obedecer si creen que la solicitud la realizó una figura de autoridad. |
| Agrado | Los humanos tienden a complacer a aquellos que se presentan como agradables o con intereses y actitudes similares. |
| Reciprocidad | Cuando se promete algo a cambio de un favor, los humanos sienten la necesidad de complacer esa deuda. |
| Coherencia | Es la tendencia a mantener la coherencia entre un compromiso público y sus acciones al respecto, por ende, se aprovecha este principio mediante la presión de sus propias palabras. |
| Validación social | Cuando otros están haciendo algo, los humanos sienten la necesidad de seguir la corriente en el afán de sentirse aceptados. |
| Escasez | Cuando la solicitud en cuestión es algo escaso o se encuentra en disputa, la gente siente la necesidad de ayudar a conseguirlo. |

**Fuente: [10].**

Es por ello por lo que, la ingeniería social representa un riesgo para los sistemas informáticos, ya que ni el mejor sistema de seguridad puede proteger la información ante un acceso otorgado por personal autorizado.

### 2.2.1 Información sensible

La información sensible dentro de un entorno empresarial se puede catalogar en dos tipos:

El **primer tipo** de información es aquella que permite el acceso a sistemas corporativos como redes institucionales o sistemas de gestión de aprendizaje; este tipo de información corresponde a las credenciales de acceso necesarias para manejar dichos sistemas. El **segundo tipo** corresponde a documentación interna y confidencial de la institución, cualquier información que no esté destinada al público general cae en esta categoría como planes de operación, proformas y nóminas.

### 2.2.2 Estructura de una técnica

Para el trabajo de investigación, se analizaron las siguientes técnicas de ingeniería social: Phishing, Spear Phishing, Pretexting, Baiting, Spoofing, Scareware y Typosquatting. El análisis de las técnicas de mitigación se organiza según un conjunto de pautas inspiradas en los principios de gestión de riesgos de seguridad de la información, compuesto por los siguientes elementos explicados en la tabla 2:

**Tabla 2:** Conceptualización de la estructura de las técnicas

| Conceptualización | Definición |
|---|---|
| Modo de operación | Describe la forma en que se materializa y se ejecuta la técnica. |
| Impacto potencial | Indica las consecuencias que la técnica podría ocasionar sobre la seguridad de la información. |

| | |
|---|---|
| Factores humanos involucrados | Comprende las vulnerabilidades psicológicas o las falencias en las políticas institucionales que permiten que la técnica logre tener éxito. |
| Medidas de prevención y mitigación | Son herramientas y sugerencias de comportamiento de los usuarios para limitar el impacto de la amenaza. |
| Tipos o Variantes de la técnica | Son variaciones en el modus operandi de la técnica que no llegan a ser técnicas diferentes. |
| Tendencias actuales | Son maneras que utilizan los atacantes para ejecutar esta técnica haciendo uso de tecnologías actuales. |

### 2.2.3 Phishing

El phishing es una técnica que utiliza la suplantación de identidad de entidades legítimas para engañar a la víctima y conseguir información sensible o acceso a sistemas [9]; los ataques mediante phishing suelen estar diseñados de tal forma que parecen mensajes genuinos de entidades legítimas enviados de forma masiva [11]; hoy en día, las técnicas de phishing se encuentran tan avanzadas al punto de que los ataques llegan a generarse de forma personalizada con información del grupo de individuos al que está dirigido para aprovecharse aún más de las víctimas y su vulnerabilidad psicológica [12]; este punto se encuentra alineado con el análisis sobre la historia del phishing realizado por Osamor et al., que destaca la facilidad con la que la información se accede online ha facilitado que los atacantes puedan explotar vulnerabilidades humanas [13].

#### Modo de operación

- **Investigación:** El atacante recolecta información sobre las víctimas, ya sea de forma legítima o no, esto con el fin de personalizar el ataque; este proceso es mucho más especializado en el spear phishing.
- **Creación del cebo:** Se diseñan correos, mensajes o sitios web que simulan ser de una entidad legítima como bancos, proveedores de servicios, empresas, etc.
- **Entrega del cebo**: El atacante envía el mensaje fraudulento a través de email, SMS, redes sociales, u otras plataformas usadas por el objetivo.
- **Captura de información:** La víctima, al creer que es una fuente legítima, proporciona datos sensibles como nombres de usuario, contraseñas, datos bancarios, etc.
- **Explotación:** El atacante hace uso de la información para cometer fraudes, acceder de forma no autorizada o ataques futuros**.**

#### Impacto potencial

- Suplantar la identidad de una persona.
- Pérdida de información sensible o filtración de información confidencial al público.
- Acceso no autorizado a sistemas empresariales sin que alguien se dé cuenta.
- Fraudes financieros y daño de la reputación de la institución.
- Deterioro grave de la imagen ante los usuarios.
- Multas y sanciones por incumplimiento de normas de protección de datos.

#### Factores humanos involucrados

- Confianza ciega en correos o comunicaciones digitales.
- Falta de verificación de remitentes.

- Urgencia emocional generada por mensajes de amenaza o promesas, por ejemplo, mensajes falsos que amenazan con perder el acceso a la cuenta.
- Curiosidad ante mensajes llamativos o alarmistas.
- Desconocimiento sobre cómo se presentan los canales oficiales de comunicación de entidades reales.

### Medidas de prevención y mitigación

- Enseñar al personal maneras para detectar correos sospechosos.
- Crear canales oficiales por donde solamente la empresa se comunique y sirva como único medio de comunicación para datos sensibles.
- Implementar la doble verificación (MFA) para añadir protección extra a las cuentas.
- Desplegar filtros avanzados de correo y herramientas de navegación segura para bloquear amenazas antes de que lleguen al usuario.
- Crear programas de pruebas que evalúen cómo los usuarios reaccionan ante las amenazas y se pueda reforzar su conocimiento actual.
- Promover la cultura de la verificación por canales adicionales antes de cualquier acción que implique transferencias de datos.

### Tipos o variantes

- **Clone phishing:** Clonar un correo legítimo y modificarlo para insertar enlaces maliciosos.
- **Whaling:** Ataques dirigidos a ejecutivos de alto nivel.
- **Pharming:** Redireccionar al usuario a un sitio web falso mediante manipulación de servidores DNS o malware.

### Tendencias actuales

- **Phishing basado en IA:** Uso de inteligencia artificial para crear mensajes más realistas y personalizados.
- **Phishing en redes sociales:** Mensajes engañosos enviados a través de plataformas como LinkedIn, Facebook o Instagram.

## 2.2.4 Spear phishing

El spear phishing es una evolución del phishing tradicional con la característica de que posee una mayor personalización durante los ataques. A diferencia del phishing tradicional, que utiliza ataques genéricos dirigidos a un gran volumen de personas, el spear phishing emplea ataques personalizados con información previamente recolectada sobre la víctima [12]. Esta técnica es altamente efectiva ya que los ataques parecen emails legítimos, y se ha demostrado que hay personas más susceptibles que otras a caer víctimas de spear phishing [7].

### Modo de operación

Según Dewan et al., el spear phishing se puede dividir en dos fases, la primera en donde el atacante intenta recolectar la mayor cantidad de información sobre la víctima con el fin de crear un escenario lo más legítimo posible, y la segunda donde el atacante usa dicha información

para incitar a la víctima a entregar información sensible mediante un correo que puede o no, contener malware [12].

## Ejemplos reales

- **Caso real:** Ataque de Spear Phishing contra el Departamento de TI de una empresa donde se recabó información personal sobre el Encargado del Departamento y se envió un mensaje aparentemente real debido a los datos mostrados en el correo.

## Impacto potencial

- Robo de credenciales y datos confidenciales del personal.
- Redirección de tráfico hacia sitios maliciosos o fraudulentos.
- Instalación no autorizada de software en los equipos de la organización.
- Acceso no autorizado a redes internas y lugares importantes de la institución.
- Fraude financiero y una grave pérdida de confianza en las instituciones víctimas del flagelo.

## Factores humanos involucrados

- **Información disponible en internet:** La información de la víctima se encuentra al alcance de los atacantes sin ninguna protección.
- **Tendencia humana a la obediencia:** La aparente legitimidad del correo hace que una orden parezca provenir de una figura de autoridad.
- **Falta de políticas de seguridad:** La falta de políticas para actuar en caso de que se soliciten datos o acceso a sistemas por correo dan pie a que ocurran este tipo de situaciones.
- **Dependencia de identificadores confiables:** Sistemas o usuarios que asumen que una IP o correo son legítimos sin realizar una verificación.

## Medidas de prevención y mitigación

- Establecer políticas sobre transferencias de seguridad que limitan qué se puede hacer por correo.
- Detectar comportamiento sospechoso en el correo.
- Identificar mails similares con ataques conocidos.

## Tendencias actuales

- Uso de modelos de lenguaje (LLM) con el fin de generar correos de forma masiva utilizando información de las víctimas.

## Indicadores de compromiso

- Estilometría del mensaje: La estilometría es la identificación de un autor mediante el análisis textual [14]; entonces, si un análisis estilométrico encuentra similitudes entre el cuerpo del mensaje y mensajes anteriores catalogados como peligrosos, se levantan alertas sobre un posible ataque.

- Análisis de las URLs y adjuntos del cuerpo: Si las URLs no se encuentran spoofeadas, o están catalogadas como potencialmente peligrosas se generan alarmas; de igual forma, el análisis de los adjuntos del correo es esencial para determinar si el correo tiene como finalidad la instalación de malware.

### 2.2.5 Pretexting

El pretexting consiste en el atacante creando un escenario falso o pretexto con el que gana un beneficio a costa de la víctima [8]. Generalmente, este método antecede a las demás técnicas, ya que mediante los escenarios falsos los atacantes plantean situaciones ideales para recolectar información de instituciones y personal, de modo que la víctima provea al atacante de información que normalmente no entregaría fuera de dicho pretexto [15]. En consecuencia, dicha recolección de datos otorga a los atacantes información para crear ataques con una mayor personalización [16].

#### Modo de operación

- El atacante recopila datos sobre el objetivo para construir un pretexto creíble como pretender asuntos internos, procesos empresariales, cambios de políticas, etc.
- Él mismo diseña una historia lo más realista posible donde el atacante asume un rol de confianza como un miembro de soporte técnico.
- El ataque puede ser mediante correo electrónico, mensajería o incluso por llamada telefónica o persona.
- Con la historia que creó pide al objetivo que proporcione credenciales, datos sensibles o que lleve a cabo acciones en sistemas informáticos.
- El atacante hace uso de la información obtenida para sus fines maliciosos.

#### Ejemplos reales

- **Caso real:** Un grupo de investigadores de seguridad descubrió cómo varios delincuentes lograban conseguir los registros de llamadas de los usuarios. El método era tan simple como alarmante: llamaban al servicio de soporte técnico de la compañía haciéndose pasar por empleados internos para solicitar los datos sin levantar sospechas.

#### Impacto potencial

- Compromete sistemas críticos o exponer información confidencial.
- Roba dinero o propiedad intelectual.
- Instala malware en la red.
- Daña la reputación de la institución.
- Abre la puerta a ataques más graves: fraudes internos, espionaje, ransomware.

#### Factores humanos involucrados

- La gente confía en autoridades: técnicos, policías, empleados bancarios.
- Los empleados amables ayudan sin realizar verificaciones de identidad.
- Nadie cuestiona si alguien es realmente quien dice ser.
- La urgencia paraliza. Si suena crítico, la gente actúa sin pensar.

- Sin procedimientos claros, nadie sabe cómo responder a solicitudes sensibles.

## Medidas de prevención y mitigación

- Cuestionar cualquier solicitud inusual, sin importar qué tan legítima o urgente parezca.
- Verificar identidad por un segundo canal: una llamada interna o en persona.
- Limitar acceso a datos. Cada persona solo maneja la información necesaria para su rol.
- Crear un canal de fácil reporte para actividades sospechosas sin riesgo a represalias.
- Hacer simulaciones de pretexting para evaluar cómo responde el equipo.
- Normalizar la verificación de la identidad y que no se catalogue como un acto de paranoia.

## Tipos o variantes

- Convencer a la víctima de que instale actualizaciones o herramientas de soporte que contienen malware.
- Pedir detalles bancarios con la excusa de actualizar la base de datos o liberar un pago pendiente.
- Suplantar auditores de seguridad o agentes de cumplimiento para pedir acceso a documentos sensibles.

## Tendencias actuales

- Usar IA para clonar voces o rostros en llamadas, esto hace un engaño mucho más creíble.
- Combinar pretexting con phishing o vishing. El atacante primero envía un email o hace una llamada para ganarse la confianza, luego atacar.

## Indicadores de compromiso

- El escenario que se plantea en el mensaje está vagamente planteado con los detalles suficientes para que una víctima con poco conocimiento del contexto caiga.
- Para darle mayor credibilidad al escenario, el atacante utilizará datos sobre la víctima con el fin de que crea que el mensaje viene de una fuente genuina; es importante recalcar que, la gran mayoría de instituciones no solicitan datos personales si no es mediante un canal seguro como webs dedicadas o archivos encriptados.

### 2.2.6 Baiting

El Baiting se basa en el ofrecimiento de un bien aparentemente inofensivo que por detrás es empleado por los atacantes como caballo de Troya [17]. Dicho bien es una carnada, de ahí su nombre en inglés, la cual engaña a la víctima para ejecutarlo, y al ejecutarse, este cebo realiza cualquier tipo de acciones maliciosas en el dispositivo o red de la víctima.

## Modo de operación

- El atacante crea un recurso atractivo para la víctima que se encuentra infectado por malware.
- El atacante distribuye este recurso mediante correos ofreciéndolo como una oportunidad única.

- La víctima cae en la trampa del atacante, interactuando con el cebo de una u otra forma.
- La víctima ve comprometida la seguridad de su equipo o red, ya sea de forma evidente o ejecutándose en segundo plano.

## Ejemplos reales

- **Caso real:** Distribución de software de pago de forma gratuita mediante email, en donde el programa en cuestión era malware que comprometió la seguridad de los equipos infectados.

## Impacto potencial

- Robo de credenciales y datos sensibles.
- Compromiso de sistemas mediante instalación de malware.
- Acceso no autorizado a redes internas.

## Factores humanos involucrados

- **Tendencia humana a aprovechar oportunidades:** Como se mencionó en las tendencias humanas básicas, cuando el pedido es algo escaso, la gente siente la necesidad de aprovechar las oportunidades.
- **Falta de políticas de seguridad:** La falta de políticas para actuar en caso de que se soliciten datos o acceso a sistemas por correo dan pie a que ocurran este tipo de situaciones.
- **Exceso de confianza en recursos adjuntos:** Confiar demasiado en recursos adjuntos abre una ventana de oportunidad para los atacantes con la que pueden aprovecharse de las víctimas.

## Medidas de prevención y mitigación

- Generar una política para asegurar la transferencia segura de información, así como limitar las acciones que se pueden realizar por correo.
- Concientizar al cuerpo universitario para que no confíen ciegamente en los adjuntos de un correo, sobre todo si proviene de fuentes no oficiales.
- Implementar sistemas de análisis para los adjuntos de un correo que detecten potencial malware.
- Implementar un sistema de detección de análisis que detecte similitudes con emails catalogados como sospechosos.

## Tipos o variantes

- **Scareware:** El scareware es un tipo de baiting que utiliza el miedo como motivo para que la víctima interactúe con el cebo, debido a la incidencia de esta técnica se analiza más adelante en el documento con mayor profundidad.

## Tendencias actuales

- **Uso de promociones existentes:** Algunas empresas ofrecen servicios con descuento para estudiantes, un atacante puede utilizar esto como oportunidad para esparcir el cebo haciéndolo pasar por un comunicado legítimo.

## Indicadores de compromiso

- Al analizar las URLs se descubre que intenta suplantar una dirección real o no cumplen con estándares de seguridad mínimos como estar vinculados a direcciones IP asociadas a dicha institución.
- Tras analizar los archivos o enlaces adjuntos del correo se los marca como potencialmente peligrosos.

### 2.2.7 Spoofing

El spoofing se puede interpretar como un engaño más que como una técnica de obtención de datos. Se define como la suplantación de identidad de una entidad legítima, de modo que la víctima confíe en la fuente y caiga en el engaño del atacante [18]. A diferencia del phishing, cuyo objetivo final es conseguir información sensible; el spoofing, tiene como objetivo final la falsificación de la identidad del remitente [19].

## Modo de operación

- El atacante elige qué tipo de identificador falsificar (IP, email, número telefónico, etc.) según el sistema o persona objetivo.
- Se modifica el campo correspondiente en el protocolo, por ejemplo, la cabecera de un paquete IP o el remitente de un correo para que parezca legítimo.
- Se envía el paquete, correo o llamada con el identificador falsificado hacia la víctima o sistema.
- La víctima o sistema confía en el identificador y responde, permitiendo al atacante interceptar información, redirigir tráfico o ejecutar acciones no autorizadas.
- El atacante puede borrar rastros o mantener acceso mediante técnicas adicionales como MITM o malware.

## Ejemplos reales

- **Caso real:** Se registró un ataque de email spoofing contra una empresa financiera. En este caso, el atacante suplantó la identidad del CEO y envió un correo electrónico donde solicitaba transferencias de dinero con carácter de urgencia.

## Impacto potencial

- Intercepción de comunicaciones con técnicas de espionaje en el medio (Man-in-the-Middle).
- Robo de credenciales de acceso, datos sensibles y otros tipos de información confidencial.
- Desviación del tráfico de usuarios a sitios maliciosos.
- Acceso no autorizado a redes privadas de la organización.

- Fraude financiero y la consecuente pérdida de confianza en la institución y el personal.
- Compromiso de sistemas por malware.

## Factores humanos involucrados

- Muchos protocolos esenciales (como ARP, DNS o SMTP) no verifican la identidad de origen de forma automática.
- El uso de comunicaciones sin cifrar facilita la interceptación y falsificación.
- Configuraciones inseguras y débiles.
- Sistemas o usuarios que dan por sentado que una IP o correo son legítimos sin verificar.
- No contar con herramientas de detección de anomalías de tráfico o de correos.

## Medidas de prevención y mitigación

- Implementar los protocolos SPF, DKIM y DMARC en el correo para asegurar la validez de los remitentes.
- Reforzar la red mediante filtrado de paquetes con sistemas IDS/IPS y ARP inspeccionado (DAI).
- Habilitar DNSSEC para autenticar respuestas DNS.
- Forzar el uso de TLS/HTTPS y autenticación multifactorial (MFA).
- Implementar sistemas de detección de anomalías en tráfico y correos.

## Tipos o variantes de la técnica

- **IP spoofing:** Falsificación de direcciones IP en paquetes de red.
- **Email spoofing:** Suplantación del remitente en correos electrónicos.
- **Caller ID spoofing:** Falsificación del número telefónico.
- **DNS spoofing:** Corrupción de registros DNS para redirigir tráfico.
- **ARP spoofing:** Suplantación de direcciones MAC en redes locales.
- **Web spoofing:** Creación de sitios web falsos que imitan a los legítimos.

## Tendencias actuales

- Uso de correos o llamadas falsas para preparar el terreno.
- Herramientas que generan masivamente correos o paquetes falsificados.
- Los atacantes aprovechan servicios legítimos para enviar correos falsos con alta credibilidad.
- Uso de técnicas para evitar la detección por filtros de spam o firewalls.

## Indicadores de compromiso

- **Ausencia de verificación de protocolos integridad:** Los protocolos pensados para asegurar la consistencia entre remitentes, clientes de correo electrónico y servidores de email se marcan como no válidos.
- **Direcciones IP asociadas no coinciden con direcciones IP conocidas:** Los dominios adjuntos en el cuerpo revelan que no están vinculados a direcciones IP asociadas a la fuente genuina.

### 2.2.8 Scareware

El scareware es una técnica fundamentada en el miedo. El ataque consiste en amenazas y alertas falsas indicando que su equipo o cuenta de usuario corren peligro y deben descargar una solución inmediatamente [8]; si la víctima hace caso a las amenazas e instala este software en su PC, su equipo se ve comprometido ya que dicho software no sirve mayor propósito que infectar la computadora o red con malware, o poner al equipo a servicio al atacante [20].

## Modo de operación

- El atacante elabora la solución falsa con un recurso comprometido o una solicitud de datos sensibles.
- El atacante distribuye la solución mediante un mensaje que infunde miedo a la víctima mediante amenazas o alertas falsas para que utilice la solución falsa y comprometa la seguridad de la información.
- La víctima cae en el engaño debido al miedo e interactúa con la solución falsa.
- La misma víctima ve comprometida la seguridad de su equipo o red ya sea de forma evidente o ejecutándose en segundo plano.

## Ejemplos reales

- **Caso real:** Emails enviados a los estudiantes de la UNACH donde se alerta de un altercado en su cuenta y se solicitan credenciales para solucionar el problema.

## Impacto potencial

- Acceso no autorizado a sistemas críticos y divulgación de información confidencial.
- Robo de datos sensibles y credenciales de acceso a sistemas.
- Redirección de usuarios a sitios maliciosos.
- Compromiso de sistemas mediante inyección de malware.

## Factores humanos involucrados

- La aparente legitimidad del correo hace que una orden parezca provenir de una figura de autoridad.
- Junto a la obediencia, el factor del miedo a perder acceso o información potencia la incidencia psicológica del mensaje.
- La falta de un análisis de recursos adjuntos en los correos dificulta que este vector se pueda mitigar.

## Medidas de prevención y mitigación

- Generar una política para limitar las acciones que puede realizar el cuerpo del correo.
- Concientizar al cuerpo universitario para que aprendan a diferenciar entre avisos reales e intentos de ingeniería social.
- Implementar sistemas de análisis para los adjuntos de un correo que detecten potencial malware.

## Tendencias actuales

- Aquellas personas que se incorporan al cuerpo estudiantil tienen más posibilidades de caer víctimas debido al desconocimiento sobre el funcionamiento de los sistemas institucionales.

## Indicadores de compromiso

Los indicadores de compromiso son similares a los del Baiting debido a que el Scareware es una variante de la técnica anterior:

- URLs del cuerpo spoofeadas o maliciosas.
- Adjuntos del cuerpo catalogados como potencialmente peligrosos.

### 2.2.9 Typosquatting

El typosquatting es un tipo de ataque que aprovecha errores tipográficos en las URL, de modo que el error pasa desapercibido por el usuario a primer vistazo [21]. Esta técnica, también llamada URL Spoofing por su componente de suplantación de un recurso legítimo, utiliza engaños simples pero efectivos al cambiar una pequeña parte de la URL que a primera vista pasa desapercibida [18]; en consecuencia, el usuario utiliza una dirección aparentemente inofensiva, pero que ya está comprometida.

## Modo de operación

- **Obtención del dominio**: El atacante consigue un dominio similar al dominio original.
- **Creación del mensaje:** El atacante genera el mensaje asemejándose a la forma original.
- **Envío del mensaje:** El atacante distribuye el mensaje desde el dominio aparentemente verídico.
- **Interacción de la víctima:** La víctima interactúa con el mensaje tomándolo como verídico al no encontrar anomalías a primera vista.

## Ejemplos reales

- **Caso real:** Un cambio de credenciales enviado por correo desde un dominio similar a microsoft: “rnicrosoft” [22].

## Factores humanos

- Acceso de personal no autorizado a sistemas críticos o ver información confidencial.
- Robo de credenciales y datos sensibles.
- Redirección de tráfico a sitios maliciosos.
- Acceso no autorizado a redes internas.
- Fraude financiero y pérdida de confianza.
- Factores Involucrados.
- Falta de verificación de protocolos de autenticación.
- Configuraciones inseguras.

## Medidas de prevención y mitigación

- **Políticas:** Generar una política para implementar herramientas de verificación de dominio.
- **Capacitación:** Concientizar al cuerpo universitario para que no confíen ciegamente en los adjuntos de un correo, sobre todo si proviene de fuentes no oficiales.
- **Análisis:** Implementar sistemas de análisis a nivel institucional para detectar URLs spoofeadas.
- **Email:** Implementar una lista negra de sitios web comprometidos, así como de potenciales sitios maliciosos.

## Tipos o variantes

- **Transposiciones de caracteres:** Se cambia la ubicación de una letra adyacente a otra. Ej.: micorsoft.com, googel.com, yuotube.com, etc.
- **Reemplazo de caracteres:** Se intercambia un carácter por otro similar, como reemplazar letras por números o caracteres de otros abecedarios. Ej.: g00gle.com donde se reemplaza la 'o' por el '0', steam.com donde se reemplaza la 'e' latina por la 'e' cirílica.
- **Adición de caracteres:** Se agrega un carácter adicional al nombre del dominio. Ej. gooogle.com, reeddit.com, yahooo.com, etc.
- **Eliminación de caracteres:** Se omite un carácter del nombre de dominio, generalmente en aquellos con nombres con letras dobles. Ej.: gogle.com, redit.com, facebok.com, etc.
- **Errores de dominio de nivel superior (TLD):** Uno o varios de los tipos anteriores se emplea sobre la última parte del nombre de dominio. Ej.: google.cm, sri.gob.es, etc.

## Tendencias actuales

- **Ataques a figuras de alto perfil:** Los ataques se enfocan en personas que tienen permisos elevados dentro de ecosistemas empresariales, por lo que son más susceptibles a ser víctimas de esta técnica.

## Indicadores de compromiso

- **Incongruencias en campos del header del email:** El protocolo de correo electrónico establece la estructura lógica de un correo indicando metadatos para asegurar la integridad del correo, anomalías en estos campos levantan alertas sobre la legitimidad del email.
- **Anomalías en las URLs adjuntas:** Un análisis a las URL adjuntas revela que no se corresponden al dominio que señalan, lo que levanta alertas sobre a donde el enlace realmente redirige.

## 2.3 Matriz de análisis de técnicas de ingeniería social

La tabla 3 corresponde a la matriz de análisis de las técnicas de mitigación, sus variables se explican a continuación.

- **El vector de ataque:** Corresponde a la identidad suplantada, el disparador psicológico y el canal del ataque.

- **Mecanismo de engaño:** Consiste en el funcionamiento técnico de la infraestructura del correo.
- **Objetivo final de la interacción:** Es lo que el ataque quiere conseguir, como robar credenciales, ejecutar malware, etc.
- **Superficie de exposición:** Explica por qué la técnica es efectiva en la institución.
- **Indicadores de compromiso:** Es el rastro que deja la técnica.

**Tabla 3:** Matriz de análisis de técnicas de ingeniería social.

| Técnica | Vector de Ataque | Mecanismo de Engaño | Objetivo Final | Superficie de Exposición | Indicadores de Compromiso |
|---|---|---|---|---|---|
| Phishing | Emails masivos | Comunicación que imita a una entidad legítima como un banco, empresas, el gobierno, etc., con enlaces y archivos adjuntos diseñados para capturar credenciales o ejecutar malware. | Robar contraseñas y datos bancarios. Pueden instalar malware y moverse lateralmente a través de la red para acceder a más sistemas. | Correo corporativo y personal, dispositivos móviles, navegadores, usuarios sin concienciación, plataformas de colaboración. | • Páginas web con direcciones engañosas<br>• Sitios web dudosos que usan certificados de seguridad recién aprobados<br>• Documentos que necesitan aprobación de macros para funcionar<br>• Enlaces que pasan por varias redirecciones antes de llegar al sitio final<br>• Aumento inusual de intentos de Login fallidos<br>• Tráfico de origen desconocido. |
| Pretexting | Correos diseñados con la intención específica de generar interacción y buscar respuesta. | Utiliza la construcción de un escenario ficticio para manipular psicológicamente a la víctima y que divulgue información o realice una acción que comprometa la seguridad del entorno. | Obtener credenciales, extraer datos confidenciales, conseguir acceso físico o autorizar transacciones fraudulentas. | Empleados internos, proveedores, personal de RRHH, entre otros. | • Solicitudes extrañas por canales poco habituales.<br>• Falta de verificación de identidad por "urgencia"<br>• Terceros con información sospechosamente detallada del personal.<br>• Llamadas o correos que presionan para conseguir datos confidenciales. |
| Spear Phishing | Escenario creado con información de la víctima. | Manipulación de la víctima usando información personal para que crea que se trata de un escenario legítimo. | Engañar a la víctima para que realice una acción en concreto. | Principalmente directivos y figuras administrativas de la institución. | • Coincidencias estilométricas entre el cuerpo del correo y mensajes anteriores catalogados como peligrosos. |
| Baiting | Escenario donde se ofrece un bien aparentemente | Aprovechar la curiosidad de la víctima para que acepte la carnada. | Ejecución de la carnada para que esta realice | Principalmente el cuerpo estudiantil. | • URLs del cuerpo spoofeadas o maliciosas. |

| | | | | | |
|---|---|---|---|---|---|
| | inofensivo como una oportunidad. | | acciones maliciosas. | | • Adjuntos del cuerpo catalogados como potencialmente peligrosos. |
| Spoofing | Mediante Red, Email o Web, buscando la imitación | Suplantación de identidad en la red: el atacante/hacker falsifica la dirección de origen para mimetizar una entidad legítima y proveer confianza. | Interceptar el tráfico de red, desviar a los usuarios hacia páginas maliciosas o evadir las listas negras. | Redes LAN, DNS público, infraestructura email y usuarios finales | • Cambios inesperados en tablas ARP<br>• DNS anómalos<br>• Diferencias discretas entre el dominio visible y el real<br>• Tráfico desde IP's desconocidas con comportamiento inusual. |
| Scareware | Cualquier escenario donde se alerte de peligro inminente y se ofrezca una solución que sea malware. | Manipulación de la víctima mediante el miedo para que realice una acción en específico. | Ejecución de la aparente solución en el equipo de la víctima. | Principalmente el cuerpo estudiantil. | • URLs del cuerpo spoofeadas o maliciosas.<br>• Adjuntos del cuerpo catalogados como potencialmente peligrosos. |
| Typosquatting | Correo enviado desde una dirección con un error tipográfico imperceptible a primera vista. | Engañar a la víctima sobre la integridad del dominio mediante un error tipográfico imperceptible a primera vista. | Engaño de la víctima para que crea en la legitimidad del origen del mensaje. | Principalmente directivos y figuras administrativas de la institución. | • Incongruencias en campos del Header del email. (Spoofing y Typosquatting) |

## Técnicas facilitadoras: Spoofing, Typosquatting y Pretexting.

Estas tres técnicas actúan como pie de apoyo para otras técnicas.

- El Spoofing y Typosquatting son técnicas complementarias que actúan como puerta de entrada para otros ataques.
- El Spoofing se aprovecha de la falta de autenticación y el Typosquatting se aprovecha de errores de tipeo.
- Junto al Pretexting, estas técnicas hacen posible que las otras técnicas tomen lugar; el Spoofing y el Typosquatting buscan suplantar una entidad legítima de una y otra forma; y el Pretexting, busca generar un contexto falso donde el engaño pueda tomar lugar.

## El vector de comunicación en Phishing, Spear Phishing y Pretexting:

Estas tres técnicas comparten el correo electrónico como vector principal, pero su mecanismo de acceso se diferencia un poco:

- El phishing y el spear phishing usan la suplantación, pero de formas muy diferentes. El phishing es masivo: envía el mismo email a miles de personas, no hay preparación. El spear phishing es dirigido: el atacante investigó a la víctima primero y usa información específica para hacer que el email parezca real.

- El pretexting es diferente porque no requiere una respuesta inmediata del objetivo, tiene como fin construir una narrativa para que el propio usuario entregue la información o rompa un protocolo de seguridad sin necesariamente depender de malware.

### El disparador psicológico en el Baiting y el Scareware:

Ambos mecanismos tienen como base provocar una reacción impulsiva ante un estímulo externo, pero con sus distinciones.

- El Baiting utiliza como carnada un beneficio o una oportunidad exclusiva, de modo que los usuarios que no quieren perder la oportunidad por miedo a quedar fuera. El Scareware, al contrario, utiliza el miedo generado por un peligro inminente o poner al equipo o la red de trabajo en riesgo.
- La diferencia radica en la emoción generada por la carnada, en el Baiting la carnada es un recurso atractivo y perder esta oportunidad genera ansiedad en la víctima; por otro lado, la carnada del Scareware es una alerta de riesgo inminente al equipo, redes internas o seguridad de los datos, lo que provoca una respuesta de miedo por motivo de autopreservación.
- Mientras que el Spoofing es una técnica puramente de suplantación, el Baiting y el Scareware son tácticas de manipulación emocional que usan el Spoofing para legitimarse.

Esta perspectiva permite ver que la ingeniería social no consiste solo en ataques aislados. Sino que es un ecosistema de técnicas que preparan el terreno para que las demás tengan éxito.

## 2.4 Marcos normativos

### 2.4.1 Marco de seguridad NIST

El marco de seguridad NIST (NIST CSF) es un documento desarrollado para ayudar a los propietarios y operadores a gestionar y reducir los riesgos de seguridad en un entorno de infraestructura crítica [23]. La figura 1 muestra las funciones del NIST CSF.


**Figura 1:** Funciones del NIST CSF.
**Fuente:** [23].

El marco detalla también niveles de implementación que describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características

definidas en el marco [23]. Además, se detallan perfiles del marco que definen resultados idóneos tras haber aplicado elementos del núcleo escogidos por la empresa según sus necesidades, estos perfiles permiten realizar un contraste entre el estado ideal y el resultado obtenido para identificar potenciales mejoras en la estructura [23]. El marco detalla seis funciones que se indican en la tabla 4.

**Tabla 4:** Funciones del NIST CSF.

| Función | Descripción |
|---|---|
| Gobernar | Establecer y supervisar una estrategia de ciberseguridad que esté alineada con la misión y los objetivos de la organización. |
| Identificar | Comprender el entorno para poder tomar decisiones informadas sobre la gestión del riesgo. |
| Proteger | Implementar las medidas necesarias para garantizar los servicios de la organización. |
| Detectar | Identificar la ocurrencia de eventos de seguridad cibernética. |
| Responder | Acciones para contener y mitigar el impacto de un incidente de ciberseguridad. |
| Recuperar | Restaurar las capacidades y los servicios que fueron afectados por un incidente. |

**Fuente:** [23].

### 2.4.2 Ley orgánica de protección de datos

En Ecuador, una ley orgánica regula el ejercicio de los derechos y garantías constitucionales [24]; de esta forma, la Ley Orgánica de Protección de Datos garantiza el derecho a la protección de datos personales en materia de acceso, decisión de información y protección mediante la regulación, prevención y desarrollo de principios, derechos y obligaciones [24]. La Universidad Nacional de Chimborazo presenta un escenario de madurez de seguridad incipiente (Nivel 1-2 del CMMI) cuyas características se detallan en la tabla 5:

**Tabla 5:** Madurez de seguridad.

| Aspecto | Estado | Riesgo |
|---|---|---|
| Políticas de seguridad | En desarrollo, se encontró que hay una consultoría en curso. | Respuestas inconsistentes, dependencia de conocimiento individual. |
| Procedimientos de respuesta a incidentes | Operativos pero informales. | Falta de escalamiento, preservación de evidencia y cumplimiento legal. |
| Automatización | Limitada, los procesos manuales son predominantes. | Tiempos de respuesta prolongados, errores humanos. |
| Cumplimiento normativo | No implementado operativamente. | Exposición a sanciones regulatorias, falta de notificaciones obligatorias. |
| Gestión de riesgos | Implícita, no documentada. | Aceptación de riesgos sin autorización ni mitigación. |

La institución necesita la formalización de su Sistema de Gestión de Incidentes de Seguridad de la Información (SGSI) alineado con estándares aceptados para una institución pública como la LOPDP para transformar las prácticas técnicas individuales en capacidades institucionales sostenibles y auditables.

## 2.5 Vulnerabilidades en entornos universitarios

Dentro de un entorno corporativo la información es el activo más valioso; de esta manera, una vulnerabilidad en los sistemas informáticos puede traer desde manchas en la reputación de la institución hasta sanciones que pueden ir desde llamados de atención, multas y en el peor de los casos penas privativas de libertad para aquellos a cargo de la seguridad de la información. Es

por este motivo que los entornos corporativos manejan con especial cuidado la seguridad de la información. Aquí toma importancia el ámbito de la ingeniería social, ya que factores externos como estrés y una gran carga de trabajo entorpecen el juicio de los usuarios, lo que los vuelve más susceptibles a ser víctimas de ataques de ingeniería social [25].

## 2.6 Diagnóstico institucional de la seguridad actual

Para la elaboración de este documento, se llevaron a cabo entrevistas con el personal de la Dirección de Tecnologías de la Información y la Comunicación (DTIC) de la UNACH. Se encontró que la gestión de recuperación de cuentas y datos sensibles se maneja mediante políticas sin formalizar y que no existen procedimientos claros para el manejo de este tipo de procesos; además, se encontró que no hay políticas claras para el manejo de la amenaza de la ingeniería social, al igual que la transferencia de información sensible por medio del correo electrónico. Con el fin de diseñar estrategias de mitigación eficaces, se llevó a cabo un levantamiento de información del entorno técnico y administrativo actual. Este análisis reveló vulnerabilidades críticas inherentes al ecosistema de la UNACH:

### 2.6.1 Ausencia de políticas formalizadas

Las entrevistas revelan una situación crítica en el entorno universitario: no existen políticas de seguridad documentadas y aprobadas internamente. El administrador del tenant de Microsoft 365 maneja las respuestas a incidentes basándose exclusivamente en criterios personales y en las recomendaciones técnicas de Microsoft, sin un marco normativo institucional que respalde sus acciones.

Aldaz mencionó en su entrevista: “Esas políticas son establecidas, no enunciadas como tal en todo, porque juntamente con el Departamento de Seguridad todavía se está trabajando una consultoría para esclarecer más ese tema” y “todavía no están como tal publicadas”. Sin procedimientos estandarizados, la respuesta ante ataques depende del criterio individual de cada administrador. Eso es un riesgo, no existen guías que mantengan la consistencia.

### 2.6.2 Procedimientos operativos Ad-hoc

A pesar de la falta de políticas formales, el entrevistado describe una serie de procedimientos reactivos que se implementan manualmente ante incidentes de phishing, malware o compromiso de cuentas. Las medidas de contención se presentan en la tabla 6:

**Tabla 6:** Medidas de contención Ad-hoc

| **Medida de contención** |
|---|
| Revocación de sesiones activas en dispositivos asociados |
| Restablecimiento de contraseñas de cuentas comprometidas |
| Eliminación de contraseñas almacenadas en aplicaciones integradas como Moodle u otras plataformas académicas |
| Activación o verificación de doble factor de autenticación (MFA) |
| Clasificación y eliminación masiva manual de correos maliciosos desde los buzones de usuarios afectados |

Estos procedimientos, si bien demuestran capacidad técnica de respuesta, son calificados explícitamente por el entrevistado como “políticas que no son mínimas, pero tampoco son avanzadas como deberían ser”.

### 2.6.3 Dependencia de herramientas de terceros

El manejo de incidentes se apoya en la tecnología de Microsoft Defender 365 y Sophos Endpoint, pero está trabajando a ciegas sin políticas que regulen aspectos clave como se explican en la tabla 7:

**Tabla 7:** Incidentes dependientes de herramientas de terceros

| **Aspectos clave sin regular** |
|---|
| Criterios de cuarentena automática e intervención manual |
| Tiempos de respuesta máximos ante incidentes |
| Protocolos de notificación a usuarios y autoridades |
| Procedimientos de preservación de evidencia forense |

El entrevistado destaca la limitación operativa: "No tenemos una herramienta [automatizada], hay otras herramientas más avanzadas que nos ayudarían a hacer automáticamente, pero obviamente tiene su costo". Esta situación evidencia que el presupuesto destinado a la seguridad limita la madurez del programa de gestión de incidentes.

### 2.6.4 Incipiente alineación con marco legal

Se identifica un esfuerzo incipiente, sin implementación operativa directa, de vincular la respuesta a incidentes con la Ley Orgánica de Protección de Datos Personales (LOPDP). El entrevistado menciona que CEDIA (Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia) promueve la inclusión de referencias legales en las comunicaciones de incidentes, pero aclara que "Eso es algo que lo estamos actualmente trabajando... No es todavía una política que ya está como tal en la Universidad" y "no se cita todavía como tal". Esta laguna es crítica dado que muchos incidentes de phishing tienen como objetivo la publicación de datos personales. Esto debería activar obligaciones específicas de notificación a la Autoridad de Protección de Datos y a los titulares afectados.

## El modelo reactivo y las limitaciones de los enlaces seguros

Los protocolos actuales dependen de la detección y los correos electrónicos maliciosos solo se identifican después de llegar a la bandeja de entrada del usuario, es ese momento en que el equipo de TI añade manualmente a los remitentes a la lista de prohibido el paso en donde crea una ventana temporal de vulnerabilidad en la que el usuario es la única barrera contra el compromiso de los datos. Los filtros dependen del proveedor. No hay seguimiento de clics ni bloqueo inmediato de URLs maliciosas para todos los usuarios.

### 2.6.5 Gestión de riesgos aceptados sin documentación

El entrevistado describe explícitamente la aceptación de riesgos no documentada: "Hay un momento que se activa que entremos en un riesgo" al otorgar excepciones temporales de 5 a 7 días para la activación del doble factor de autenticación a usuarios que no disponen de teléfono móvil. Esta práctica, si bien responde a necesidades operativas reales, carece de: 1) Evaluación formal de riesgo; 2) Aprobación de autoridades competentes; 3) Registro de excepciones; y 4) Plan de mitigación compensatoria durante el período de vulnerabilidad aumentada.

### Canal de denuncia silencioso

La universidad tiene un mecanismo de denuncia a través del correo "mesadeayuda@unach.edu.ec", pero se encontró una falta de difusión o formación sobre este canal. Un mecanismo de denuncia que es desconocido por la base de usuarios es equivalente a no tener nada, lo que conduce a una grave falta de denuncia de incidentes.

### 2.6.6 Colaboración externa sin acuerdos formalizados

La gestión de incidentes involucra mantener una colaboración con CEDIA para análisis de vulnerabilidades y aspectos legales pero el entrevistado no menciona la existencia de acuerdos de confidencialidad ni protocolos de comunicación de incidentes o definición de responsabilidades entre las entidades, lo que puede comprometer la cadena de custodia de evidencia y la claridad en la respuesta coordinada.

### 2.6.7 Asimetría en la conciencia sobre seguridad

La defensa humana de la institución está fragmentada. En 2025 se llevó a cabo una iniciativa obligatoria de ciberseguridad para el personal administrativo y docente; sin embargo, se encontró que no existe una estrategia paralela para el conjunto estudiantil como se indica en el anexo 12. Dado que los estudiantes son frecuentemente objetivos de estafas y ataques de phishing, esta omisión representa la mayor superficie de ataque no supervisada dentro de la red de la universidad.

## 2.7 Arquitectura de mitigación propuesta

En respuesta a las deficiencias identificadas en el Diagnóstico de la Seguridad, se propone una serie de políticas pensadas para mitigar las incidencias de la ingeniería social en el sistema de correos electrónicos; junto a la proposición de las políticas, se suman sugerencias para mecanismos de análisis de correos y manejo de direcciones de correo maliciosas, además de protocolos de acción ante ataques de ingeniería social.

### Políticas de manejo para el correo electrónico

Las políticas se componen del enunciado y su justificación de ser. Para clasificar las políticas, se las agrupa según su finalidad:

- Formar en el uso del sistema de correos.
- Asegurar su uso correcto.
- Manejar información y datos sensibles.
- Manejar las incidencias de ingeniería social.

### Mecanismos de análisis de correos y manejo direcciones maliciosas

Los sistemas de análisis para ingeniería social provistos por la propia Microsoft se salen del presupuesto asignado para el sistema de correo electrónico. Para solucionar este problema, se plantean mecanismos y procedimientos en alineación con las políticas planteadas:

- Creación de un canal oficial para reportes de ataques.
- Mecanismo del canal oficial.
- Ciclo de vida de un reporte.
- Clasificación de remitentes según la incidencia de los ataques.

- Clasificación de remitentes a una lista negra.
- Tratamiento de direcciones en la lista negra.
- Perfilado de correos maliciosos.
- Clasificación de correos maliciosos.
- Generación de perfiles mediante clustering para su clasificación automática.

## Protocolos de acción

Los protocolos de acción son la manera de operar del departamento de TI ante una incidencia de ingeniería social. Para el sistema de correos electrónicos se elaboraron dos protocolos: Para accionar ante ataques apartados y ante ataques reincidentes.

## 2.8 Estrategias de mitigación contra la ingeniería social

Kevin Mitnick explica en su libro "El arte de la Intrusión" los factores que hacen posible la ingeniería social, señalando que la naturaleza humana es el principio que utilizan los atacantes para vulnerar sistemas informáticos [10]. Así mismo, Mitnick señala políticas para mitigar la incidencia de la ingeniería social en el ámbito corporativo total; para este trabajo, se tomó como punto de partida las políticas que se pueden extrapolar al entorno corporativo de los correos electrónicos.

Las políticas desarrolladas en este trabajo se encuentran en los resultados.

### 2.8.1 Políticas y protocolos de seguridad

Se deben establecer políticas de seguridad claras y precisas para mitigar las incidencias de los ataques de ingeniería social [10]. En base a las normativas, se generan protocolos que rigen cómo se debe manejar el proceso de la seguridad de los datos en el sistema de correos, de este modo se asegura el cumplimiento de las políticas con procesos que minimizan el riesgo de caer víctima de la ingeniería social. Una cosa para tener en cuenta sobre las políticas es que a medida que la tecnología avanza se deben ir actualizando a la par para que no queden obsoletas.

### 2.8.2 Formación en concienciación

La primera línea de defensa ante la ingeniería social son los propios usuarios; puesto que, un ataque de ingeniería social pasa desapercibido por software antimalware convencional; son los propios usuarios los que deben notar anomalías y reportar incidentes al administrador de red [10]. Se puede concluir entonces que, los usuarios deben estar capacitados para detectar dichas anomalías en el sistema de correos institucional; por ello, es que es necesaria la formación en concienciación sobre técnicas de ingeniería social para que el usuario sirva como primera línea de defensa y sepa protegerse de correos potencialmente maliciosos y reporte los correos que le parezcan sospechosos.

### 2.8.3 Simulaciones de ataques

Una simulación de ataques de phishing sirve para verificar el estado de la preparación de los usuarios ante la amenaza de la ingeniería social. Los datos obtenidos de la simulación se recogen por el personal del DTIC para detectar debilidades en la red de usuarios y cómo se pueden mitigar, además de conocer los puntos débiles a capacitar. Otra ventaja de las

simulaciones de phishing es que mantienen alerta a los usuarios de cómo puede verse un ataque y qué medidas tomar al respecto si se llega a ser víctima, este modelo de aprendizaje "al momento" demuestra ser útil a la hora de educar ya que el impacto de haber caído resulta efectivo en cómo los usuarios manejan la situación en un futuro [7]. En base a los resultados de las simulaciones, se deben realizar auditorías de seguridad puesto que ningún sistema es completamente invulnerable; de esta forma, se detectan incidencias que van a poder ser gestionadas, y se obtienen datos nuevos para actualizar las políticas y capacitaciones en base a los hallazgos encontrados.

# CAPÍTULO III. METODOLOGÍA

## 3.1 Tipo de investigación

Para el presente trabajo de investigación se escogió un enfoque mixto, de corte longitudinal, con alcance aplicado y explicativo.

Se escogió el enfoque mixto porque se utilizó una combinación de técnicas cualitativas como el análisis documental y entrevistas para elaborar el análisis de las técnicas de ingeniería social y la evaluación de la efectividad de las estrategias desarrolladas; y técnicas cuantitativas, como la implementación de cuestionarios piloto y el desarrollo de un cuasiexperimento de naturaleza Pretest-Postest.

El cuasiexperimento consistió en una simulación de phishing con grupo de control y experimental e intervención; contempla las fases Pretest con la primera oleada de correos maliciosos, intervención mediante un programa de capacitación para el grupo experimental y un intervalo de 15 días para eliminar el sesgo de aprendizaje, y Postest con la segunda oleada de correos maliciosos para evaluar los cambios en ambos grupos bajo ambas condiciones; debido a la cronología del cuasiexperimento, se establece una temporalidad longitudinal a raíz de que se realizaron mediciones en dos momentos distintos.

El alcance de la investigación se define como aplicado, dado que se centra en el desarrollo de una solución a una problemática institucional; y también como explicativo, ya que busca una relación entre la intervención y la reducción de riesgos en el sistema de correos.

## 3.2 Diseño de la investigación

El presente estudio se desarrolló bajo un diseño cuasiexperimental con Pretest y Postest y grupo de control. Se eligió el diseño cuasiexperimental ya que se empleó un muestreo no probabilístico por conveniencia debido a las limitaciones de acceso a la población a raíz de las autorizaciones por parte del DTIC para la realización del cuasiexperimento y la necesidad de mantener un control riguroso sobre la intervención [26].

Los hallazgos conseguidos tras el cuasiexperimento son de gran valor para el desarrollo de la seguridad informática en la institución, pero debido a la limitación que representó una población tan reducida, no se pretende que se puedan generalizar los resultados a toda la universidad, sino que sirvan como indicadores para las tendencias en el comportamiento de los sujetos de estudio.

## 3.3 Población de estudio y tamaño muestral

Para la recolección de datos con respecto al estado de las políticas de correo institucionales, correspondiente al apartado conceptual del trabajo, se realizaron entrevistas al director del DTIC y al ingeniero a cargo del correo institucional; y para el componente experimental, la población de estudio estuvo comprendida por directivos, empleados y estudiantes de la facultad de Ciencias Políticas y Administrativas de la UNACH que utilizan el correo institucional.

Para la ejecución de los cuestionarios piloto, se escogió una muestra de 20 sujetos divididos en dos grupos de 10 sujetos clasificados en perfiles técnicos y no técnicos en materia de informática. Por otro lado, para el desarrollo del cuasiexperimento con mediciones Pretest y Postest, se determinó una muestra de 30 sujetos distribuidos equitativamente mediante un muestreo no probabilístico por conveniencia. Con respecto a la distribución de los grupos, los sujetos que participaron en los cuestionarios piloto no fueron los mismos que los participantes del cuasiexperimento; y los 30 sujetos de estudio fueron distribuidos de manera equitativa en un grupo de control (Grupo A) y un grupo experimental (Grupo B) de 15 sujetos, respectivamente.

La dimensión muestral de los sujetos elegidos para el cuasiexperimento se puede justificar según los criterios de Sampieri et al. [26], donde se establece que, en diseños experimentales o cuasiexperimentales, un mínimo de 15 sujetos por grupo es aceptable para garantizar la viabilidad y el control riguroso de las variables independientes. Así mismo, autores como Montgomery y Runger [27] consideran que un tamaño muestral de n=30 es el mínimo recomendable para propósitos prácticos en el ámbito de la ingeniería y ciencias aplicadas.

Para el presente caso de estudio, es fundamental que los grupos de estudio del cuasiexperimento se encuentren en igualdad de condiciones; de modo que, para validar este criterio se realizó un análisis de diferencias entre grupos mediante la Prueba Exacta de Fisher, ya que no requiere muestras grandes para ser precisa [28]. Para evaluar el impacto del programa de capacitación, se aplicó la Prueba de McNemar para medir los cambios ocurridos en los grupos antes y después de la intervención, ya que según Vidakovic, la prueba de McNemar es la mejor para realizar inferencias en tablas pareadas con intervenciones realizadas sobre los mismos sujetos [28].

De este modo, la combinación de un diseño controlado y el uso de estadística exacta asegura la confiabilidad de los hallazgos para identificar cómo la formación en ciberseguridad incide en la capacidad de los usuarios para mitigar ataques de ingeniería social.

## 3.4 Técnicas de recolección de datos

Para el desarrollo del trabajo de titulación, se llevó a cabo la extracción, revisión y análisis de literatura científica, reportes de la industria de TI y normativas vigentes, lo que permitió definir y analizar las técnicas de ingeniería social y sentar las bases para el diseño de las estrategias de mitigación. Acto seguido, se aplicaron cuestionarios piloto y una serie de entrevistas como fuentes primarias de información; la encuesta fue distribuida a una muestra aleatoria con perfiles técnicos y no técnicos sobre tecnología para medir su percepción del riesgo y conocimiento normativo; y las entrevistas se centraron en obtener información técnica detallada por parte del personal del DTIC de la UNACH. Los cuestionarios general y técnico se presentan en los anexos 2 y 3.

Para el cuasiexperimento, se realizó una simulación de phishing por correo electrónico en dos etapas distintas donde al grupo experimental se lo sometía a un programa de capacitación antes de la segunda etapa con el fin de analizar el impacto que tendría el programa de capacitación. Si un usuario era parte del grupo de control y enviaba datos a través de la página de phishing, no ocurría nada; pero si formaba parte del grupo experimental, la página de

recopilación de credenciales redirigía a los usuarios que introducían datos a una página de destino de aprendizaje al momento; esta página reproducía inmediatamente los videos correspondientes a la capacitación valiéndose del shock del usuario para proporcionar una retroalimentación correctiva instantánea; por el contrario, los usuarios del grupo de control que interactuaron con la simulación no eran redirigidos a esta página, por lo que no eran sometidos a la capacitación.

El repositorio del programa de capacitación se evidencia en el anexo 6, la configuración de la herramienta para la simulación en el anexo 10 y los datos en bruto del cuasiexperimento en los anexos 7 y 8 la interpretación se encuentra en la sección de resultados.

En la tabla 8 se detallan las técnicas de recolección de datos.

**Tabla 8:** Técnicas de recolección de datos.

| Técnica | Tipo | Descripción | Aplicación en el trabajo |
|---|---|---|---|
| Revisión de literatura | Secundaria | Recopilación, extracción y análisis de información de documentos existentes que contengan datos relevantes para la investigación. | Revisión de libros, revistas con factor de impacto, reportes de industria, y normativa correspondiente para la definición y análisis de las técnicas de ingeniería social y las estrategias de mitigación. |
| Encuesta | Primaria | Serie de preguntas cerradas dirigidas a un grupo de participantes para recolectar información sobre conocimientos y actitudes sobre ingeniería social. | Aplicación de un cuestionario a una muestra aleatoria de la población con perfiles técnicos y no técnicos en materia de informática para evaluar su nivel de concienciación, conocimiento de políticas de seguridad y percepción del riesgo ante la ingeniería social. |
| Entrevista | Primaria | Interacción donde el investigador formula preguntas a un experto para obtener información detallada sobre el tema de estudio. | Ejecución de una serie de entrevistas al personal del DTIC para conocer la normativa vigente en la institución y las prácticas que se llevan a cabo en el sistema de correos electrónicos. |
| Cuasiexperimento | Primaria | Manipulación de variables independientes para conocer sus efectos sobre variables dependientes con un grupo de estudio escogido a conveniencia. | Ejecución de una simulación de phishing controlada sobre un grupo experimental y de control, seguida de una intervención y la segunda simulación, con el fin de medir la efectividad de las estrategias de mitigación sobre la muestra de estudio. |

## 3.5 Consideraciones éticas

El trabajo de investigación se realizó con la autorización del DTIC en un entorno controlado para la toma de datos. Se garantizó la privacidad y confidencialidad de la información mediante la anonimización de los datos, eliminando identificadores directos (nombres, cédulas, correos) y aplicando codificación alfanumérica a cada registro. El trabajo de titulación se elaboró con la condición de que ningún tipo de información personal se difundiera en el trabajo de modo que los resultados se presentaron de forma agregada evitando la identificación individual como se evidencia en los anexos 4, 5, 7 y 8.

Se respetaron los criterios de seguridad de la información ya que no se recopiló ningún tipo de información que permita identificar a los sujetos que formaron parte de las encuestas y el cuasiexperimento, además, tras la elaboración del trabajo de investigación, se eliminaron los datos que pudieran llevar al reconocimiento de los sujetos minimizando el riesgo de identificación individual. La metodología consideró el valor de los hallazgos sobre el riesgo asociado al estudio, lo que llevó a considerar que divulgar la participación en la investigación podía comprometer la validez de los resultados; por ende, este trabajo adoptó un enfoque de intervención controlada exclusivamente orientado a fines académicos e investigativos. El desarrollo de la investigación no implicó exposición a riesgo mayor al que se expone una persona en su diario vivir, ni comprometió la salud física o psíquica de los participantes.

## 3.6 Métodos de análisis y procesamiento de datos

Para el procesamiento de los datos recolectados y la evaluación de la efectividad de las estrategias de mitigación se aplicó un enfoque de análisis mixto alineado con el diseño cuasiexperimental.

### 3.6.1 Análisis cuantitativo

El análisis cuantitativo se realizó mediante estadística descriptiva e inferencial para el análisis de los datos obtenidos de las encuestas y los resultados de las simulaciones de ataques.

#### Estadística descriptiva

Se utilizó para la agrupación y organización de los datos en bruto obtenidos directamente de las técnicas cuantitativas de recolección de datos. Se empleó Excel para la tabulación de datos y análisis inicial.

En primera instancia, la caracterización de los resultados de la prueba piloto permitió conocer las vulnerabilidades iniciales, las respuestas de los cuestionarios se encuentran en los anexos 4 y 5. A continuación, el resumen de los resultados del cuasiexperimento permitió conocer los panoramas antes y después del programa de capacitación en ambos grupos, los datos en bruto del cuasiexperimento se encuentran en los anexos 7 y 8. Ambas interpretaciones se encuentran en los resultados.

#### Estadística inferencial

Se utilizó para elaborar contrastes de hipótesis entre lo obtenido del cuasiexperimento a partir de los datos recolectados; para la realización de las pruebas estadísticas, se utilizó el lenguaje R.

Primero, se utilizó la Prueba Exacta de Fisher para determinar si los grupos del cuasiexperimento eran equivalentes al inicio de la simulación; y después, se empleó la Prueba de McNemar para la validación de la efectividad de las estrategias a partir de los estados anterior y posterior al programa de capacitación. Las pruebas de hipótesis se encuentran en los resultados.

### 3.6.2 Análisis cualitativo

El análisis cualitativo tuvo como fin interpretar las causas y contextos que explican los resultados. Para ello, se utilizaron los siguientes métodos:

## Análisis de contenido documental

Se aplicó durante la revisión de la literatura a lo largo del marco teórico y la elaboración de las estrategias de mitigación. En principio, se utilizó para el análisis de las técnicas de ingeniería social que amenazan el entorno de correo electrónico de la UNACH; del mismo modo, se utilizó para la elaboración de las estrategias de mitigación.

## Análisis de discurso

Se utilizó para evaluar las entrevistas realizadas al personal del DTIC en el marco teórico con el objetivo de conocer las normativas y procedimientos vigentes que rigen al sistema de correos de la UNACH, este análisis precedió a la elaboración de las estrategias ya que recolectó información sobre procedimientos de mitigación que los encargados del DTIC mantenían sin registro formal. Las transcripciones de las entrevistas se encuentran en los anexos 11 y 12.

# 3.7 Hipótesis

Para validar la equivalencia entre los grupos de la población al inicio del cuasiexperimento, y evaluar los cambios antes y después de la intervención se plantearon las siguientes hipótesis en función de la prueba estadística que se usó para su análisis.

Las hipótesis para comprobar la **equivalencia entre grupos al inicio de la simulación** empleando la prueba exacta de Fisher para todas las variables del cuasiexperimento, en este caso de estudio, se construyen de la siguiente manera:

- H0: Las proporciones de sujetos en la muestra son independientes del grupo.
- H1: Las proporciones de sujetos en la muestra no son independientes del grupo.

Las hipótesis para comprobar **cambios en los grupos antes y después de la intervención** mediante la prueba de McNemar para todas las variables del cuasiexperimento antes y después de la intervención se construyen de la siguiente manera:

- H0: No existe un cambio significativo en la proporción de variables entre ambas mediciones.
- H1: Existe un cambio significativo en la proporción de variables entre ambas mediciones.

# 3.8 Identificación de variables

## Variable dependiente

## Efectividad de la protección de datos personales y corporativos

Esta variable representa el resultado o el efecto que se desea medir. Se conceptualiza como la capacidad de las medidas implementadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información que se maneja en los sistemas de correo empresarial de la UNACH.

En este trabajo de titulación, la efectividad se mide acorde la cantidad de usuarios que fueron capacitados para mitigar una incidencia de ingeniería social. Se considera que una estrategia es efectiva cuando la combinación de políticas claras y concienciación humana minimiza exitosamente el riesgo de un ciberataque basado en ingeniería social.

### Variable independiente

### Políticas de seguridad y estrategias de mitigación

Esta variable corresponde al factor que se manipula directamente en el cuasiexperimento para observar su impacto sobre la protección de datos. En este trabajo de titulación, la variable independiente corresponde a la intervención aplicada sobre el grupo experimental. La variable se fundamenta en la implementación de las estrategias diseñadas tras la prueba piloto y se desglosa en los siguientes componentes:

- Programa de capacitación técnica sobre riesgos de ingeniería social.
- La difusión y aplicación de políticas de seguridad robustas que gobiernan el comportamiento de los usuarios del sistema de correo electrónico institucional.

## 3.9 Operacionalización de variables

La tabla 9 presenta la operacionalización de variables

**Tabla 9:** Operacionalización de las variables.

| Problema | Tema | Objetivos | Variables | Conceptualización | Dimensión | Indicadores |
|---|---|---|---|---|---|---|
| ¿Cómo influyen las técnicas de ingeniería social y estrategias de mitigación en la efectividad de la protección de datos personales y corporativos en sistemas de correo empresariales? | Técnicas de ingeniería social y estrategias de mitigación para la protección de datos personales y corporativos en sistemas de correo empresariales. | **General**<br>Analizar las técnicas de ingeniería social y desarrollar estrategias de mitigación basadas en formación y políticas de seguridad para proteger los datos personales y corporativos en los sistemas de correo empresariales. | **Independiente**<br>Políticas de seguridad y Estrategias de mitigación. | Conjunto de tácticas y controles para poder contrarrestar ataques basados en la manipulación psicológica. Combinan la formación y concienciación del personal, el establecimiento de políticas de seguridad robustas y el uso de tecnologías [29]. | Seguridad | • Exposición al programa de capacitación. |
| | | **Específicos**<br>• Identificar y analizar las principales técnicas de ingeniería social que amenazan la seguridad de los datos en los sistemas de correo electrónico institucional de la UNACH, mediante revisión de literatura y análisis de casos locales.<br>• Diseñar e implementar estrategias de mitigación no invasivas, como programas de formación en ciberseguridad y políticas de seguridad, para fortalecer la protección de datos en los sistemas de correo electrónico de la UNACH, sin modificar la infraestructura de Microsoft 365.<br>• Evaluar la efectividad de la protección de datos personales y corporativos aplicando las técnicas de ingeniería social y estrategias de mitigación, utilizando el marco de seguridad NIST CSF y la LOPDP. | **Dependiente**<br>Efectividad de la protección de datos personales y corporativos. | Se mide por su capacidad para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Una estrategia es efectiva cuando combina controles técnicos, políticas claras y concienciación humana para minimizar riesgos y prevenir brechas [30]. | Efectividad | • Cantidad de correos maliciosos abiertos.<br>• Cantidad de clics en enlaces maliciosos.<br>• Cantidad de datos enviados mediante el correo malicioso.<br>• Cantidad de reportes de correos maliciosos. |

## 3.10 Metodología de desarrollo

El presente trabajo empleó una estructura metodológica investigativa de carácter aplicado y explicativo de corte longitudinal dividida en cuatro fases bajo un enfoque mixto comprendidas por el diagnóstico, diseño, implementación y evaluación de una intervención estratégica centrada en la formación y políticas de seguridad mediante un diseño de investigación cuasiexperimental [31].

La estructura metodológica consta de cuatro fases principales, las cuales se alinean con el diseño cuasiexperimental del proyecto y están orientadas a cumplir de manera sistemática los objetivos específicos establecidos [32]. Para crear las fases del desarrollo, se tomó como base el trabajo de Kothari [31] y se adaptó cada etapa a las necesidades del trabajo de titulación. El detalle de la estructura consta en la tabla 10.

**Tabla 10:** Fases de la metodología investigativa para el trabajo de investigación.

| Fase | Objetivo |
|---|---|
| Diagnóstico institucional | Realizar el análisis de las técnicas de ingeniería social mediante revisión de literatura, y el levantamiento de información técnica del sistema de correo electrónico universitario mediante entrevistas al personal y cuestionarios piloto para determinar la situación actual de la institución. |
| Diseño del cuasiexperimento y desarrollo de activos | Desarrollar las estrategias de mitigación y políticas de seguridad, el programa de capacitación, y los instrumentos de recolección de datos necesarios para las fases Pretest y Postest del cuasiexperimento. |
| Implementación de la intervención | Ejecutar el despliegue de la investigación mediante el Pretest a los grupos de estudio, seguido de la ejecución del programa de capacitación en el grupo experimental. |
| Evaluación de los resultados | Aplicar el Postest a los grupos de estudio y realizar un análisis estadístico comparativo para determinar el impacto del programa de capacitación en la mitigación de ataques de ingeniería social. |

**Fuente:** Adaptado según el trabajo de Kothari [31].

### 3.10.1 Fase 1: Diagnóstico institucional

En esta fase se desarrollaron las bases teóricas y diagnósticas de la investigación; para ello, primero, se realizó la revisión de literatura pertinente a las técnicas de ingeniería social y normativa vigente sobre tratamiento de datos personales y seguridad en sistemas informáticos; y para el apartado del diagnóstico institucional, se elaboró el levantamiento de información técnica al sistema de correo electrónico mediante entrevistas al personal del DTIC para conocer la situación del manejo del sistema de correo y cuestionarios piloto a los 20 sujetos según sus perfiles técnicos y no técnicos para identificar el nivel de conocimiento de la población sobre la ingeniería social.

#### Revisión de literatura

Se realizó una revisión sistemática de artículos académicos y reportes de industria para la clasificación de las técnicas de ingeniería social como se menciona en los apartados 2.1 y 2.2. También, se realizó una revisión literaria para conocer los marcos normativos sobre los cuales el trabajo de titulación tomó como base para generar las estrategias como se menciona en el

apartado 2.3, y en el apartado 2.4, la revisión correspondiente a conocer las vulnerabilidades que los entornos universitarios afrontan con los sistemas de correo electrónico.

### Levantamiento de información técnica

Primero, se llevaron a cabo entrevistas semiestructuradas con los responsables del DTIC con el objetivo de trazar un mapa del panorama técnico. Las entrevistas revelaron información esencial para la elaboración de políticas y estrategias de mitigación. El análisis realizado a las entrevistas se evidencia en el apartado 2.5 y la transcripción de las entrevistas se encuentra en los anexos 11 y 12.

### Aplicación del cuestionario piloto

Para culminar con la fase de diagnóstico institucional, se elaboraron cuestionarios dirigidos a dos perfiles de sujetos de estudio, sujetos con conocimiento técnico de tecnologías de la información y sujetos sin dicho conocimiento. El propósito de recolectar datos fue conocer la situación de la población con respecto a la ingeniería social. Los participantes de los cuestionarios piloto fueron independientes de la muestra del cuasiexperimento. El análisis de las respuestas de los cuestionarios figura en los resultados. Los cuestionarios general y técnico se encuentran en los anexos 2 y 3, y sus respectivas respuestas en los anexos 4 y 5.

## 3.10.2 Fase 2: Diseño del cuasiexperimento y desarrollo de activos

Corresponde al Objetivo Específico 2 y consiste en el diseño del programa de capacitación. En esta fase se crearon los entregables estratégicos y corresponde al desarrollo de las estrategias de mitigación y políticas de seguridad a partir del análisis de las técnicas de ingeniería social y el diagnóstico institucional.

### Desarrollo de estrategias de mitigación y políticas de seguridad

La investigación permitió estructurar una propuesta de mitigación dividida en dos ejes: El primero consistió en una arquitectura de políticas explicada en el apartado 2.6, donde se detalla cómo se van a manejar las amenazas en el sistema de correo institucional; y el segundo, un plan de acción ante la amenaza de la ingeniería social explicado en el apartado 2.7. Las políticas y las estrategias elaboradas a partir de las propuestas anteriores se encuentran en los resultados.

## 3.10.3 Fase 3: Implementación de la intervención

La fase de implementación corresponde a la parte práctica del cuasiexperimento; para su desarrollo, se llevó a cabo la primera simulación de phishing para toda la muestra y la aplicación del programa de capacitación al grupo experimental en caso de que el usuario llegara a enviar credenciales a través del enlace.

### Primera simulación de phishing

Durante este paso, se envió la primera oleada de correos maliciosos a los sujetos de estudio de ambos grupos. La herramienta GoPhish se encargó de recolectar los datos correspondientes al Pretest.

Se utilizó la herramienta GoPhish para la simulación y Excel para la tabulación de datos; en esta herramienta, se crearon plantillas de phishing utilizando la marca oficial de la UNACH y suplantando la identidad de Google para poner a prueba la capacidad de los usuarios para detectar discrepancias visuales. La especificación de la plantilla utilizada para cada sujeto de ambos grupos se encuentra en el anexo 7 y la configuración de la herramienta GoPhish se encuentra en el anexo 10. Mediante la simulación, se recogieron los datos sobre cada incidencia explicados en la tabla 11.

**Tabla 11:** Variables del cuasiexperimento

| Variable | Indicador | Valores |
|---|---|---|
| Abierto | ¿El usuario abrió el correo? | (Sí/No) |
| Clic | ¿El usuario hizo clic en el enlace malicioso del correo? | (Sí/No) |
| Datos | ¿El usuario envió datos a través del enlace malicioso? | (Sí/No) |
| Reportado | ¿El usuario reportó el correo? | (Sí/No) |

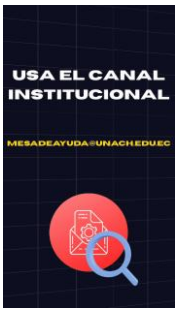
## Difusión del programa de capacitación

Para mitigar la brecha entre la política escrita y el comportamiento de los usuarios frente a ataques de ingeniería social, se elaboraron cuatro videos educativos e instructivos a modo de programa de capacitación. La premisa de los videos fue la función Detectar del NIST CSF. Para la redacción de los guiones, se hizo hincapié en las técnicas de ingeniería social que pueden atacar al conjunto estudiantil y corporativo, así mismo como acciones que se deben llevar a cabo. La producción de los videos empleó un formato dinámico y rápido que presenta la información de la forma resumida pero clara; el motivo de escoger este formato de producción fue la necesidad de aprovechar el shock inicial del usuario priorizando los conceptos importantes por sobre los detalles y la capacidad de reproducción automática del contenido multimedia.

El programa de capacitación se realizó de forma automatizada y diferenciada entre ambos grupos. Aquellos que pertenecían al grupo de control (A) y enviaban datos mediante el enlace adjunto no recibían la capacitación; mientras que los sujetos del grupo experimental (B) que sí interactuaban con el enlace de la misma forma, eran redirigidos a una página donde los videos se reproducían a modo de capacitación. Esta forma de retroalimentación correctiva por shock permitió que los usuarios recibieran el programa de capacitación de forma instantánea al momento de la transgresión.

La tabla 12 muestra la premisa de los videos y el enlace al repositorio de los videos se encuentra en el anexo 6:

**Tabla 12:** Videos correspondientes a la capacitación

| Premisa del Video | Captura |
|---|---|
| Introducción a la ingeniería social y definición de phishing y pretexting junto a recomendaciones para no caer en ataques de ingeniería social. |  **Figura 2:** Captura del video 1. |
| Definición de baiting y spoofing y recomendación de la verificación por otro canal para comprobar mensajes sospechosos. |  **Figura 3:** Captura del video 2. |
| Definición de scareware y typosquatting junto a recomendaciones de seguridad ante estas técnicas. |  **Figura 4:** Captura del video 3. |
| Difusión del canal de reportes “mesadeayuda@unach.edu.ec” |  **Figura 5:** Captura del video 4. |

## 3.10.4 Fase 4: Evaluación de los resultados

Para la fase final del desarrollo de la investigación, se aplicó la segunda simulación 15 días después de la primera oleada de correos maliciosos para reducir el sesgo de aprendizaje. De nuevo, la herramienta GoPhish recolectó los datos correspondientes al Postest con la misma configuración de la etapa anterior, el detalle de las plantillas utilizadas para la segunda etapa se encuentra en el anexo 8.

## Segunda simulación de phishing y evaluación de los datos

Tras recolectar los datos finales, se realizó la evaluación mediante un análisis estadístico comparativo con el fin de determinar el impacto del programa de capacitación en la mitigación de ataques de ingeniería social.

El análisis estadístico consistió en pruebas de hipótesis. Primero, se evaluó la independencia de los grupos en el Pretest mediante la Prueba Exacta de Fisher con el fin de determinar si se encontraban en igualdad de condiciones al inicio del cuasiexperimento. Acto seguido, se realizó la Prueba de McNemar para contrastar los resultados del Pretest y Postest con el fin de analizar el impacto del programa de formación y la efectividad de las estrategias. Una vez completado el análisis estadístico, se realizó una evaluación mediante la interpretación de los valores estadísticos para explicar por qué las estrategias demostraron un determinado nivel de efectividad. Los análisis estadísticos y la interpretación de los valores se encuentran en los resultados.

## 3.11 Modelado de la investigación

En la figura 6 se indica la línea de tiempo de las fases de la investigación mediante el diagrama de Gantt respectivo.

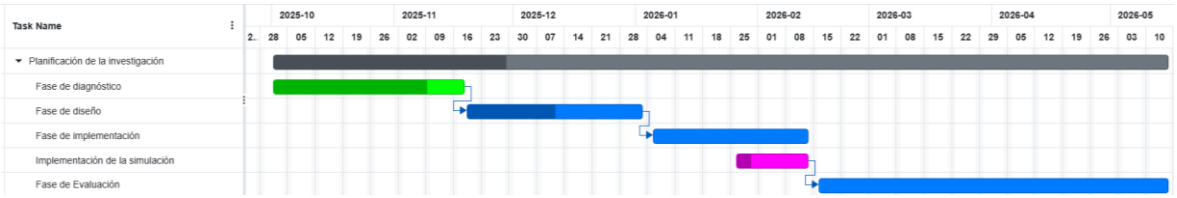



**Figura 6:** Diagrama de Gantt del cronograma de investigación.

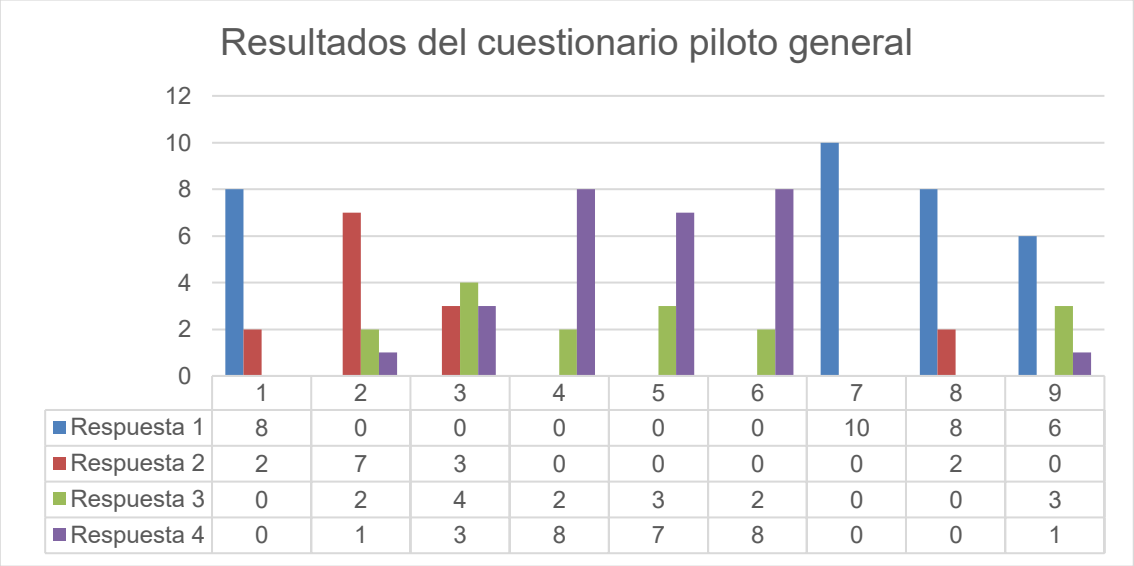
# CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

## 4.1 Resultados

### 4.1.1 Resultados de los cuestionarios piloto

Como sustento teórico para la elaboración de las estrategias de mitigación y políticas de seguridad, se realizó una revisión de literatura y un levantamiento de información técnica que consistió en una serie de entrevistas y cuestionarios dirigidos a una muestra de la población con perfiles técnicos y no técnicos en materia de informática, independientes de la muestra del cuasiexperimento.

Los resultados del cuestionario piloto aplicado a sujetos con perfil no técnico se muestran en la figura 7.



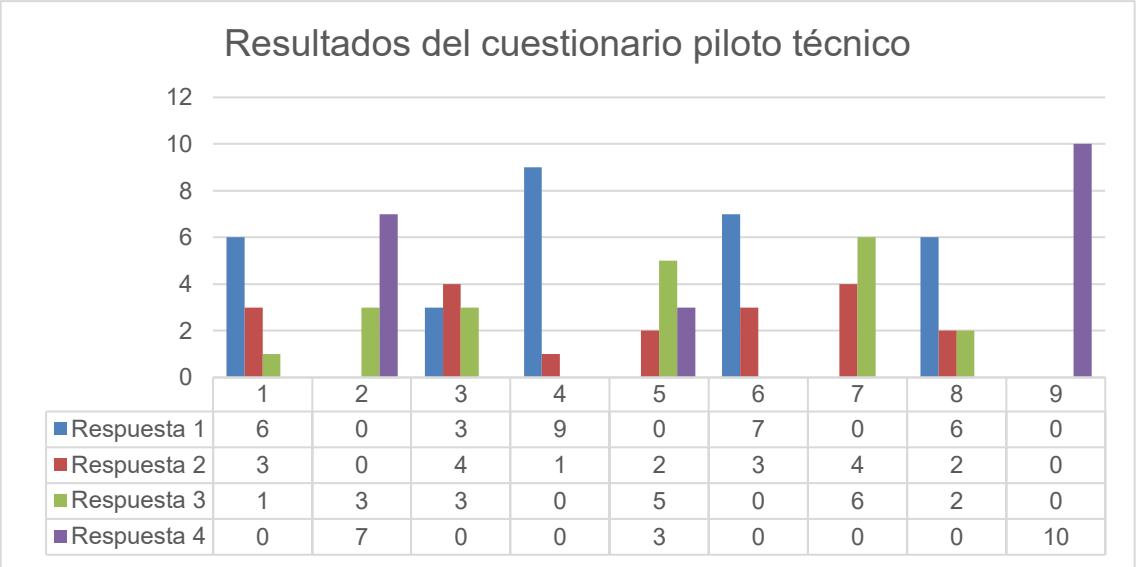

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| Respuesta 1 | 8 | 0 | 0 | 0 | 0 | 0 | 10 | 8 | 6 |
| Respuesta 2 | 2 | 7 | 3 | 0 | 0 | 0 | 0 | 2 | 0 |
| Respuesta 3 | 0 | 2 | 4 | 2 | 3 | 2 | 0 | 0 | 3 |
| Respuesta 4 | 0 | 1 | 3 | 8 | 7 | 8 | 0 | 0 | 1 |

**Figura 7:** Resultados del cuestionario piloto general.

Una vez obtenidas las interpretaciones individuales, se generaron los siguientes resultados:

- Gran parte de la población confía en sus habilidades para no caer en un engaño; sin embargo, una mayoría de usuarios no reporta haber detectado señales de alarma evidentes, lo que lleva a la creencia de que una parte significativa de la población es una víctima potencial de ataques de ingeniería social.
- Las técnicas de ingeniería social analizadas representan una amenaza al sistema de correo, sobre todo el Phishing, Pretexting, Spoofing, Scareware y Typosquatting, lo que indica que se debe aplicar especial cuidado al tratar estos casos.
- Se necesita promover campañas de concientización en ciberseguridad y hacer hincapié en la difusión de los canales de denuncia al cuerpo universitario.

Los resultados del cuestionario piloto aplicado a sujetos con perfil técnico se muestran en la figura 8.




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| Respuesta 1 | 6 | 0 | 3 | 9 | 0 | 7 | 0 | 6 | 0 |
| Respuesta 2 | 3 | 0 | 4 | 1 | 2 | 3 | 4 | 2 | 0 |
| Respuesta 3 | 1 | 3 | 3 | 0 | 5 | 0 | 6 | 2 | 0 |
| Respuesta 4 | 0 | 7 | 0 | 0 | 3 | 0 | 0 | 0 | 10 |

**Figura 8:** Resultados del cuestionario técnico.

Mediante la interpretación se generaron los siguientes resultados:

- Se necesita de forma urgente políticas y procedimientos claros, definidos y formalizados para responder ante la amenaza de la ingeniería social.
- A criterio del personal técnico, las amenazas de ingeniería social más latentes son el Spear Phishing, Spoofing y Typosquatting.
- La política impulsada por Microsoft de la doble autenticación es una barrera eficaz para minimizar el robo de credenciales, pero el resto de las herramientas que Microsoft provee no son suficientes para mitigar todos los riesgos.

### 4.1.2 Políticas y Estrategias de mitigación para la protección de datos personales y corporativos en el sistema de correos electrónico institucional.

En el marco institucional de la UNACH, la incidencia de los ataques mediante ingeniería social en el sistema de correos electrónicos representa una amenaza para la integridad de la seguridad de los sistemas de TI institucionales, así como para la información y seguridad de los datos de la comunidad universitaria. El presente documento plantea una serie de estrategias y políticas no invasivas que buscan proteger la integridad de los sistemas de TI, así como la seguridad de la información.

## Propuesta

Se plantean políticas preventivas y predictivas para manejar la seguridad del entorno de correos electrónicos.

A partir de las políticas, se plantea la creación de un sistema de análisis de correos electrónicos mediante clustering para la generación de perfiles de ataques.

También, se plantea el ciclo de vida de los correos reportados como sospechosos, modo de proceder, clasificación de su remitente y modo de proceder por parte del departamento de TI.

Además, se plantea la creación de una vía directa de reportes para incidencias de ingeniería social, de modo que todo miembro de la comunidad universitaria pueda reportar incidentes o correos sospechosos sin necesidad de comunicarse con el departamento de TI como intermediario.

Finalmente, se plantean protocolos correctivos para tomar acción ante ataques apartados y ataques reincidentes.

## Políticas de manejo para el correo electrónico

Según la investigación realizada, existen seis técnicas de ingeniería social que amenazan a la institución: Phishing, Pretexting, Baiting, Spoofing, Scareware y Typosquatting.

Para prevenir y mitigar las incidencias de ingeniería social se plantean las siguientes políticas:

## Políticas de formación general

- Todas las personas dentro de la institución deben someterse a una capacitación u orientación de ciberseguridad. Así mismo, se deberán impartir capacitaciones o campañas para refrescar dicho conocimiento.
- **Justificación:** Todas las personas deben tener bases en materia de ciberseguridad que deben estar actualizándose constantemente.

- Todo el personal y los usuarios deberán completar la formación en ciberseguridad antes de que se les habiliten sus cuentas de correo electrónico.
- **Justificación:** Una comunidad universitaria bien capacitada es mucho menos vulnerable a los engaños y ataques de ingeniería social.

## Políticas de uso del sistema de correo electrónico

- Todas las peticiones de soporte deberán ser tratadas exclusivamente por el personal del departamento de TI.
- **Justificación:** No se debe garantizar acceso a terceros a los sistemas institucionales en ninguna circunstancia.

- Una solicitud para crear un correo electrónico solo podrá ser ejecutada si es autorizada por el jefe del departamento de TI.
- **Justificación:** Solo el personal del DTIC debe ser capaz de gestionar asuntos correspondientes al sistema de email institucional.

- Todo correo recién creado tendrá una contraseña por defecto que deberá ser cambiada apenas el usuario reciba acceso al correo.
- **Justificación:** Solo el usuario final tiene derecho a conocer sus credenciales de acceso y no debe ser conocido por ninguna otra persona, incluida la institución.

- Deberá haber un número de intentos de acceso limitado antes de bloquear el acceso a la cuenta definitivamente, para revertir el bloqueo se deberá solicitar el cambio de contraseña en el departamento de TI.
- **Justificación:** Limitar el número de intentos previene ataques de fuerza bruta.

- Para deshabilitar un correo, solo el jefe de TI puede autorizar, y solo si hay una razón válida.
- **Justificación:** Una cuenta es un activo de la institución, para su inhabilitación solo el director a cargo del sistema de correos institucional podrá autorizar su inhabilitación.

- La contraseña debe contener mínimo 12 caracteres incluyendo mayúsculas, minúsculas, números y símbolos.
- **Justificación:** Una contraseña distintos caracteres es mucho más difícil de vulnerar que una con un mismo tipo de caracteres.

- Las contraseñas deberán tener un tiempo de vida antes de solicitar un cambio de contraseña.
- **Justificación:** Asegurar que las contraseñas caduquen fuerza a los usuarios a reestablecer su contraseña dificultando ataques por robo de credenciales antiguas.

- Las contraseñas nunca deberán ser divulgadas a ningún miembro de la comunidad universitaria o terceros.
- **Justificación:** La cuenta de correo es única para cada persona, solo su propietario debe manejar la cuenta, así como sus credenciales de acceso.

- Ningún usuario debe tener la capacidad de deshabilitar su correo en ninguna circunstancia.
- **Justificación:** Solo el personal administrativo debe tener la potestad de inhabilitar cuentas, y solo cuando haya una razón justificable.

- Ningún miembro del personal administrativo debe compartir información sensible sin antes verificar la información del destinatario.
- **Justificación:** El personal administrativo, antes de compartir información sensible con otro miembro de la administración, debe verificar que efectivamente se trate del destinatario correcto.

## Políticas de manejo de información sensible o acciones sobre sistemas informáticos

- No comunicar información sensible a correos no institucionales o que sean de orígenes cuestionables.
- **Justificación:** La información no debe ser compartida a terceros no autorizados, esto se evita limitando el contacto con direcciones no institucionales y aquellas que carezcan de certeza sobre su finalidad.

- No comunicar detalles de los sistemas informáticos a ningún correo que no sea una dirección confiable y verificada.
- **Justificación:** No compartir datos con personas o plataformas externas asegura que la información privada de la organización no termine en manos equivocadas.

- Cualquier correo proveniente de una fuente confiable que solicite información sensible o alguna acción sobre los sistemas informáticos necesita de confirmación adicional mediante una vía adicional aparte del correo.
- **Justificación:** A pesar de ser una fuente confiable, no se debe descartar la posibilidad de que la cuenta esté comprometida, de modo que el propietario de la cuenta deberá confirmar que solicitó esta información para considerar la solicitud como auténtica.

- Ningún tipo de información sensible deberá ser enviada sin haberse encriptado, y la clave de desencriptado deberá ser compartida por otro medio.
- **Justificación:** En caso de que la información sea interceptada, el atacante no podrá hacer nada sin la clave para desencriptar la información.

## Políticas para el manejo de incidencias

- Se deberán reportar todos los incidentes al departamento de TI, estos incidentes pueden ser, pero no se limitan a: Phishing, Spoofing, Pretexting, Baiting, Scareware, Typosquatting y Spear-Phishing.
- **Justificación:** Todo incidente debe ser reportado al departamento de TI para su posterior documentación.

- Se deberán documentar todos los incidentes.
- **Justificación:** Sin registro, los patrones no se detectan. Un incidente aislado parece accidente; diez documentados pueden revelar un ataque coordinado.

- Se deberán documentar las direcciones del origen del incidente, tanto de correo como direcciones IP asociadas.
- **Justificación:** La documentación de incidentes y direcciones de origen, sirven para armar una base de conocimientos de atacantes y modos de ataque.

- Se deberán reportar todas las direcciones, tanto de correo como IP, que parezcan sospechosas.
- **Justificación:** Las direcciones sospechosas se marcan para seguimiento activo por parte de TI. Cualquier comportamiento anómalo queda registrado y puede atenderse antes de que escale.

- Se deberán analizar todos los incidentes.
- **Justificación:** El análisis de las incidencias de ingeniería social permite mejorar el nivel de alerta del departamento de TI para futuros casos.

## Estrategias de mitigación

## Creación de un canal oficial para reportes de ataques

Es necesario que exista una vía oficial de reportes de incidentes donde tanto directivos, empleados, docentes y estudiantes puedan reportar incidentes y no se deba depender de un intermediario o una vía de reporte no segura.

Actualmente, existe algo similar en el área de "Mesa de Ayuda" en el departamento de TI, ya que el personal se puede acercar y reportar actividad sospechosa; además, el departamento cuenta con una dirección de correo para atender los requerimientos; Sin embargo, la vía oficial que se plantea redirige los correos maliciosos a un contenedor especial donde son aislados para su análisis en lugar de ser manejados por el departamento de ayuda.

## Propuesta de estructuración

La vía oficial deberá ser una dirección de correo electrónico, que reciba los mensajes y los almacene en un contenedor aislado del entorno de correo institucional.

El ciclo de vida de los correos partirá en los usuarios reenviando los correos que identificaron como maliciosos a la dirección oficial de reportes, después, los usuarios deberán eliminar el correo malicioso de su bandeja de entrada. Dicho correo, una vez recibido mediante el canal de reportes, se almacenará en un contenedor aislado del entorno de correo institucional a la espera de ser analizado tanto por un sistema de detección de fraude y de ser necesario, contar con la revisión de parte de un encargado, una vez terminada la revisión, el correo se eliminará del contenedor, ya sea automáticamente por el sistema de detección o manualmente por el delegado a cargo de la revisión.

## Clasificación de remitentes según la incidencia de los ataques

Un atacante puede usar direcciones de correo externas a la universidad o direcciones internas secuestradas. Debido a que las direcciones internas no pueden registrarse directamente en una lista negra porque pertenecen a un miembro de la comunidad universitaria se propone el siguiente sistema de clasificación para direcciones externas y direcciones institucionales.

## Lista negra

Corresponde a todas las direcciones que hayan tenido comportamiento sospechoso o hayan intentado un ataque.

## Tratamiento de direcciones en la lista negra

Las direcciones que sean agregadas a la lista negra se podrán retirar solamente si pertenecen a un miembro de la comunidad universitaria; caso contrario, las direcciones externas, al ser ajenas a la universidad, no aportan al funcionamiento de la institución, por tanto, se puede prescindir de estas.

El modo de proceder consistirá en enviar un correo reportando comportamiento extraño y solicitando que el responsable del correo se presente en el departamento de TI para tratar el asunto; si tiempo después no existe respuesta de parte del responsable de la dirección, se intentará contactar con el responsable del correo por otros medios para que se acerque al departamento de TI; si después de haber entablado contacto no hay respuesta del responsable, el departamento de TI iniciará un proceso para investigar el percance notificando que se llevará a cabo dicha acción. Si no llega a haber respuesta del responsable dentro de un plazo razonable, o en la investigación se demuestra que el propietario de la cuenta fue consciente de que realizaba acciones maliciosas, se procederán a tomar acciones disciplinarias en contra del responsable acorde al código de convivencia de la institución.

## Perfilado de correos maliciosos

La institución actualmente traslada los correos maliciosos a una bandeja de spam o los elimina en los casos más riesgosos.

Esta forma de operar es poco eficiente ya que depende de la revisión humana para determinar qué es spam y qué es riesgoso, resulta una carga de trabajo adicional para los encargados de manejar el sistema de correo electrónico y, no genera conocimiento para manejar situaciones futuras similares.

Debido a esto, la propuesta de la creación de perfiles surge debido a la necesidad de un tratamiento con mayor profundidad para las incidencias de ingeniería social, es por ello por lo que se plantea la creación de perfiles de correos maliciosos para que existan referencias a la hora de clasificar y tratar este tipo de incidencias.

## Propuesta de protocolo de clasificación

Los correos deberán ser analizados para obtener una secuencia de patrones que se puedan asociar a una técnica de ingeniería social u otra.

El sistema de análisis de correos se creará mediante técnicas de clustering para agrupar los correos según patrones en común, estos serán los perfiles, de modo que, al recibir un nuevo incidente, este se clasifique automáticamente.

Para esto, se necesitará un conjunto de correos maliciosos previamente aislados del entorno institucional.

Acto seguido, se deberán aplicar las técnicas de clustering para agrupar a los distintos correos según sus patrones; dichos resultados, se almacenarán en una base de conocimientos que servirá para el análisis automático de los ataques subsiguientes.

## Protocolos de acción correctivos

## Acción ante ataques apartados

Para este tipo de ataques, se debe proceder colocando la dirección del remitente en la lista negra para evitar futuras incidencias; después, analizar el contenido del correo para poder clasificar al ataque, si no llega a haber coincidencias con la base de conocimientos, se deberá esperar a la revisión manual. Queda a veredicto del encargado de la revisión registrar el correo en la base de conocimientos.

## Ataques reincidentes

Para este tipo de ataques, se debe proceder colocando las direcciones de los remitentes en la lista negra para evitar futuras incidencias; además, se deberá investigar si hay direcciones IP asociadas a los correos, para agregarlas a la lista negra; después, analizar el contenido del correo para poder clasificar al ataque, si no llega a haber coincidencias con la base de conocimientos, se deberá esperar a la revisión manual. Queda a veredicto del encargado de la revisión registrar el correo en la base de conocimientos.

## 4.1.3 Resultados del programa de capacitación e impacto en el cuasiexperimento

Con las variables que se registran de los usuarios, ABIERTO, CLIC, DATOS y REPORTADO, se procedió a evaluar el estado de los grupos al inicio de la simulación y los cambios entre ambos grupos después del programa de capacitación.

## Prueba de independencia

Primero, se evaluó que ambos grupos se encuentren en igualdad de condiciones al inicio del cuasiexperimento mediante un análisis de asociación entre las variables ABIERTO, CLIC, DATOS y REPORTADO, empleando la Prueba Exacta de Fisher. Los resultados de la prueba se detallan en la tabla 13.

**Tabla 13:** Resultados de la Prueba Exacta de Fisher.

| Variable | Valor P |
|---|---|
| Clic | 1.00 |
| Abierto | 1.00 |
| Datos | 1.00 |
| Reportado | 1.00 |

La figura 9 presenta la región de rechazo para cada variable en la prueba de Fisher:

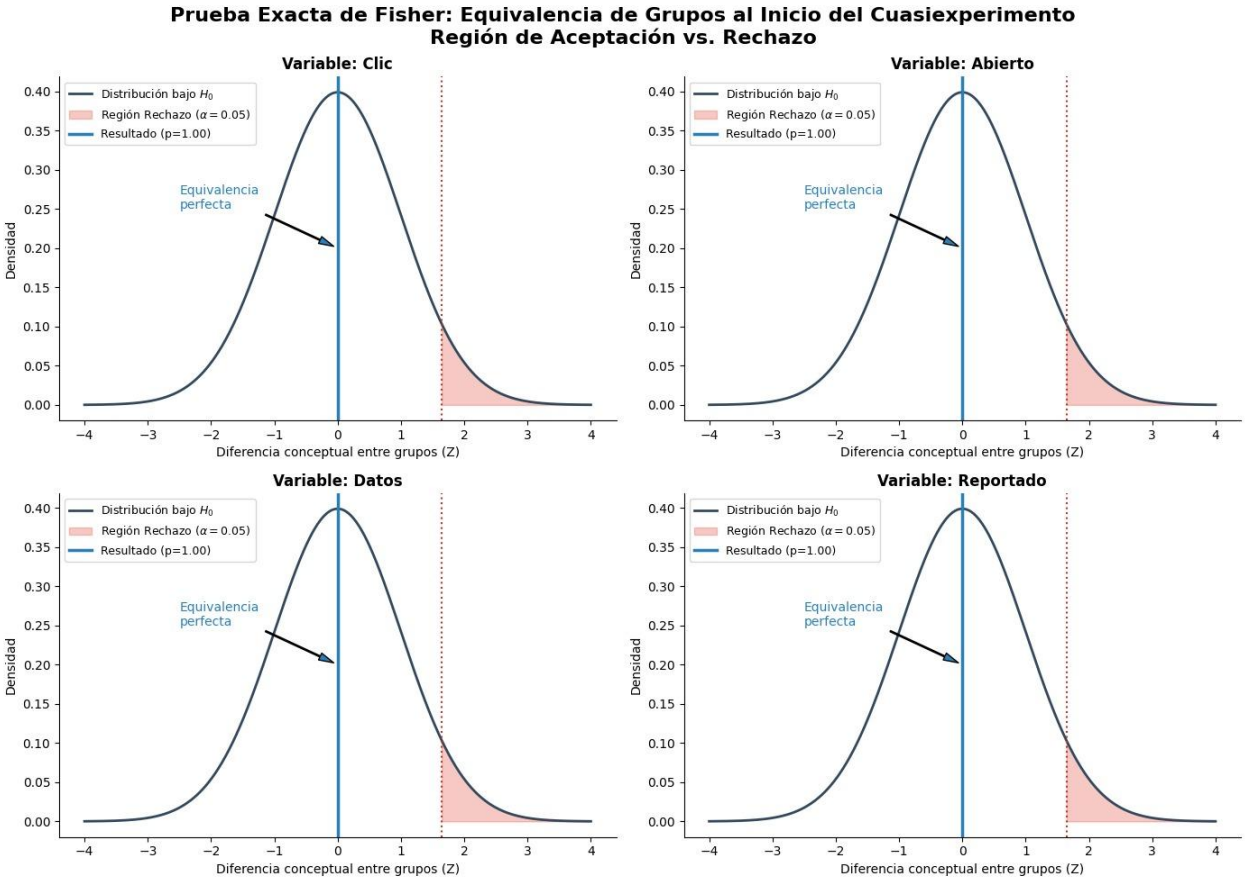



**Figura 9:** Región de rechazo para las variables en la prueba de Fisher

Con un nivel de significancia establecido de $\alpha = 0.05$, la regla de decisión indica que si $p \leq \alpha$, entonces se rechaza la hipótesis nula. El valor (p=1.00) no cumple ese criterio en ninguna de las variables, así que no se rechaza la hipótesis nula. Entonces, existe evidencia para afirmar que las proporciones son independientes del grupo, lo que indica que no existieron diferencias significativas; en consecuencia, al inicio del cuasiexperimento los grupos eran equivalentes, hecho que resulta crucial el momento de aplicar un diseño con grupo de control.

## Prueba de McNemar

Al inicio, se realizó la primera oleada de emails maliciosos; de forma inmediata, se aplicó la capacitación y 15 días después para mitigar el sesgo de aprendizaje, se realizó la segunda oleada de correos maliciosos. La tabla 14 presenta los valores de significancia obtenidos mediante la prueba de McNemar para cada variable.

**Tabla 14:** Resultados de la prueba de McNemar, se marca con un * los valores P menores a la significancia.

| Variable | Valor P (Grupo A) | Valor P (Grupo B) |
|---|---|---|
| Clic | 0.1824 | 0.0736 |
| Abierto | 1.0000 | 0.6171 |
| Datos | 0.4795 | 1.0000 |
| Reportado | 1.0000 | 0.0026* |

Con un nivel de significancia establecido de $\alpha = 0.05$, la regla de decisión indica que si $p \leq a$, se rechaza la hipótesis nula, lo que determina los resultados que se muestran en la tabla 15.

La figura 10 presenta la región de rechazo para cada variable:

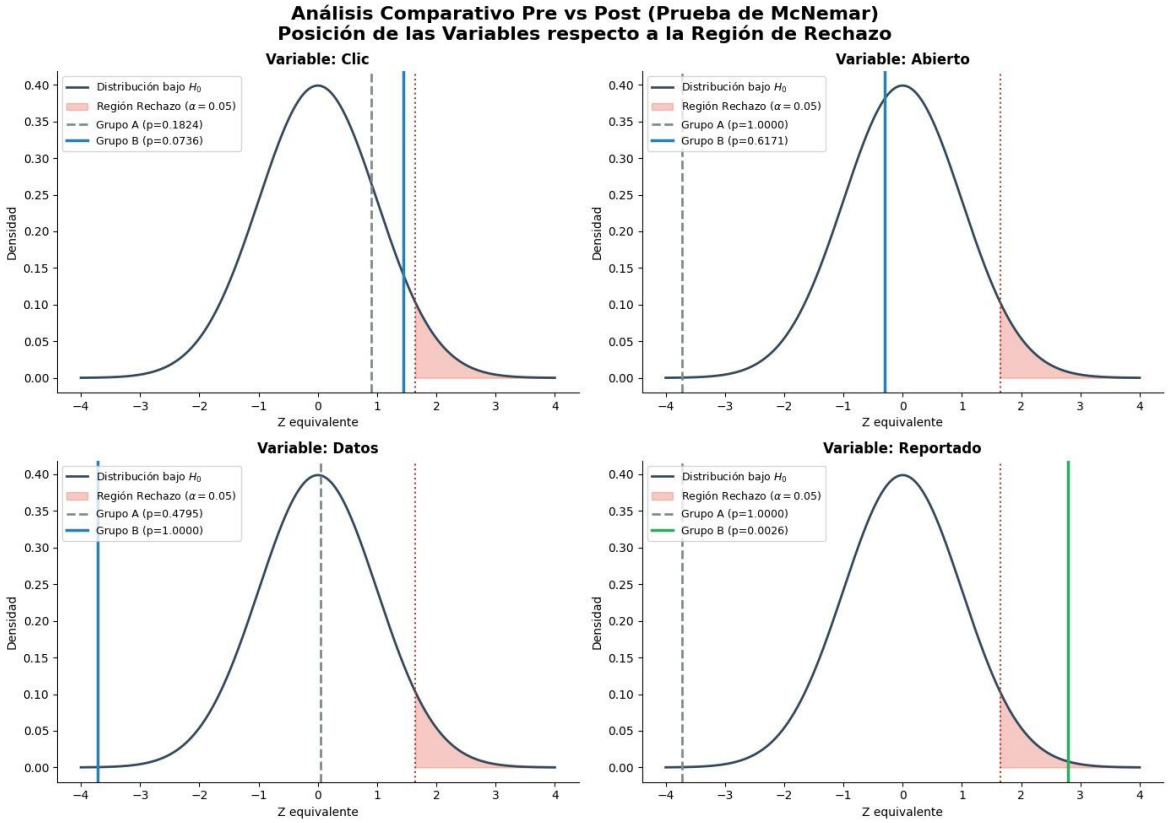



**Figura 10:** Región de rechazo para las variables en la prueba de McNemar.

**Tabla 15:** Decisión para cada variable según el grupo.

| Variable | Decisión para el grupo A | Decisión para el grupo B |
|---|---|---|
| Clic | No se rechaza la hipótesis nula | No se rechaza la hipótesis nula |
| Abierto | No se rechaza la hipótesis nula | No se rechaza la hipótesis nula |
| Datos | No se rechaza la hipótesis nula | No se rechaza la hipótesis nula |
| Reportado | No se rechaza la hipótesis nula | Se rechaza la hipótesis nula |

Los resultados indican que en el grupo A no se rechaza la hipótesis nula en todas las variables, lo que indica que no hubo cambios significativos después del Postest. Este resultado es de esperarse puesto que el grupo de control no recibió la capacitación por obvias razones.

Por el contrario, en el grupo B no se rechaza la hipótesis nula en las variables Clic, Abierto y Datos; pero en la variable Reportado sí, lo que sugiere que no hubo cambios en dichas variables tras el Postest, pero sí hubo un cambio altamente significativo que no se le puede atribuir al azar en la cantidad de usuarios que reportaron los correos.

## Análisis estadísticos

Las tablas de contingencia permiten conocer más a detalle el comportamiento de los usuarios en el cuasiexperimento ya que se pueden ver los cambios en bruto, dentro de la diagonal principal de la matriz se señalan los perfiles de estabilidad, usuarios que mantuvieron su conducta inicial como activos o inactivos; y las celdas restantes, detallan los perfiles cambiantes, aquellos que pasaron de activos a inactivos y aquellos que pasaron de inactivos a activos. Las tablas de contingencia de todas las variables para todos los grupos se detallan en el anexo 9:

Para el grupo A, la variable "Clic" presentó un cambio destacable ya que 7 usuarios dejaron de hacer clic en el correo y 2 cliquearon a pesar de no haberlo hecho en el pasado. En la variable "Abierto", 2 usuarios dejaron de abrir el enlace del correo y 1 lo abrió a pesar de no haberlo hecho con anterioridad. Para la variable "Datos", se puede destacar que 2 usuarios enviaron datos y lo dejaron de hacer. Y en la variable "Reportado", no hubo cambios en el comportamiento del grupo, pero se puede destacar que 2 usuarios mantuvieron su comportamiento de reportar correos maliciosos.

Para el grupo B, la variable CLIC presentó un cambio en que 5 usuarios dejaron de hacer clic en el correo y no hubo usuarios que no hicieran clic y luego lo hicieran. En la variable ABIERTO, 3 usuarios dejaron de abrir el enlace del correo y 1 lo abrió a pesar de no haberlo hecho con anterioridad. Para la variable DATOS, 1 usuario dejó de enviar datos y 1 usuario envió datos en ambas situaciones. Y en la variable REPORTADO, hubo el cambio más significativo en el comportamiento de 11 usuarios que reportaron el correo cuando antes no lo hicieron, se debe destacar que hubo 1 usuario que reportó en ambas ocasiones.

## Análisis por dimensiones de comportamiento

### 1.- Apertura de correos electrónicos sospechosos

En el grupo de control (Grupo A), dos participantes dejaron de abrir correos sospechosos y uno comenzó a hacerlo. El valor (p=1.0000) indica la ausencia de evidencia estadística suficiente para afirmar que el el programa de capacitación modificó este comportamiento significativamente.

Respecto a la variable ABIERTO, en el grupo experimental (Grupo B), 3 sujetos dejaron de abrir correos maliciosos, mientras que 1 inició esta conducta. La prueba de McNemar indicó un valor (p=0.6171), lo cual permitió concluir que no existieron diferencias estadísticamente significativas en la proporción de apertura de correos entre ambas mediciones en ausencia de programa de capacitación.

Por tanto, el programa de capacitación no demostró un efecto considerable sobre la reducción de la apertura de correos phishing.

### 2.- Susceptibilidad al clic en enlaces maliciosos

En el de control (Grupo A), siete participantes dejaron de hacer clic en enlaces maliciosos y dos comenzaron a hacerlo. Los números parecen favorables, pero la prueba de McNemar arrojó un valor (p=0.1824), por lo que no es estadísticamente significativo y no podemos atribuir el cambio al programa de capacitación.

En la condición experimental (Grupo B), se observó una tendencia favorable hacia la reducción del comportamiento de riesgo: 5 participantes que habían efectuado clic en el Pre-Test dejaron de hacerlo en el Post-Test, mientras que ningún sujeto que se había abstenido inicialmente desarrolló dicho comportamiento en la segunda medición. No obstante, el valor obtenido en la prueba de McNemar ($p=0.0736$) no alcanzó el umbral de significancia estadística convencional, aunque evidencia una tendencia que podría deberse a factores ajenos a la intervención como la interacción entre usuarios.

Se concluye entonces que el programa de capacitación no redujo significativamente la tendencia a hacer clic en enlaces maliciosos.

## 3.- Compromiso de datos sensibles

La métrica crítica correspondiente al envío de credenciales o información que puede llegar a ser confidencial no mostró cambios sustanciales en ninguna de las dos condiciones. En el Grupo A, dos sujetos dejaron de exponer datos, pero de igual forma sin alcanzar significancia estadística ($p=0.4795$). Estos resultados sugieren que, tanto en presencia como en ausencia de la estrategia de capacitación, no se produjo una modificación estadísticamente relevante en la conducta impulsiva asociada al ingreso de información en plataformas malintencionadas.

En el Grupo B, un único participante dejó de comprometer sus datos, sin que se registraran casos de adopción de este comportamiento de riesgo ($p=1.000$).

Con respecto al comportamiento de los usuarios, se puede hablar de un perfil susceptible a siempre enviar datos, ya que como se evidenció en la tabla de contingencia de la variable DATOS del grupo B, un mismo usuario siempre envió datos, lo que vuelve a este perfil de usuario en particular una víctima perfecta para ataques de ingeniería social.

## 4.- Reporte de correos electrónicos sospechosos

El hallazgo más importante del trabajo se observa en la variable REPORTADO. En el Grupo A no se registraron cambios en esta variable entre ambas mediciones ($p=1.000$), manteniendo estables las conductas de reporte observadas en el momento inicial.

Por el contrario, en el Grupo B, once participantes que no reportaban correos sospechosos en el Pretest iniciaron esta práctica en el Postest, mientras que ningún sujeto que reportaba en un principio dejó de hacerlo. La prueba de McNemar arrojó un valor ($p=0.0026$), lo cual indica una diferencia estadísticamente muy significativa ($p< 0.01$).

El resultado del grupo B permite afirmar que el programa de capacitación fue efectivo para incrementar significativamente las tasas de reporte de amenazas hacia el canal de reportes.

## 4.1.4 Síntesis de los hallazgos

La revisión del documental del marco teórico permitió formular un análisis sobre las técnicas de ingeniería social que afectan a los sistemas de correo electrónico de manera general. El levantamiento de información técnica del sistema de correo institucional mediante las entrevistas al personal de DTIC y el conocimiento de las debilidades del sistema de correo

electrónico institucional, y junto a las respuestas del cuestionario piloto, facilitaron formular las políticas y estrategias de mitigación para la protección de datos personales y corporativos en el sistema de correo electrónico institucional con respecto a la evidencia de la falta de políticas de seguridad institucionales formalizadas.

De manera posterior, se elaboró un programa de capacitación según la función DETECTAR del NIST CSF creado a partir de las políticas y estrategias que a su vez se utilizó a modo de intervención en el cuasiexperimento; los resultados obtenidos a raíz de comparar el comportamiento entre el grupo de control y experimental permitieron evaluar la efectividad de las estrategias donde los resultados demuestran que:

- Las conductas de riesgo, como el compromiso de datos, apertura de correos y clic en enlaces maliciosos permanecieron sin modificaciones estadísticamente relevantes en la condición de control y experimental en el cuasiexperimento.
- El programa de capacitación produjo un efecto estadísticamente significativo en la dimensión proactiva de reporte de correos sospechosos para el grupo experimental ($p=0.0026$).

Lo que lleva a pensar que las técnicas de ingeniería social son una amenaza ante la protección de datos personales y corporativos en el sistema de correo electrónico como es el caso del sistema institucional; además, el estado administrativo y funcional del sistema de correo electrónico institucional facilita que las técnicas de ingeniería social penetren en la capa de protección debido a la falta de concienciación del cuerpo universitario.

Por otro lado, las políticas y estrategias influyen en la reducción de comportamientos proactivos como reportar los correos mediante el canal institucional; pero, no influyen en la reducción de los comportamientos de riesgo pasivos como hacer clic en enlaces, abrir correos electrónicos y facilitar credenciales; de modo que, es correcto afirmar que existe una tendencia a la efectividad parcial de las políticas y estrategias en la protección de datos personales y corporativos en sistemas de correo empresariales.

## 4.2 Discusión

Las estrategias de mitigación quedaron como propuesta debido a que su integración requería un proceso administrativo de modificación de políticas internas de la institución; a pesar de ello, el documento quedó como precedente para el desarrollo de futuras estrategias que la institución por parte del DTIC, lo cual servirá para fortalecer la estructura de la seguridad de los datos personales y corporativos en la institución.

El estudio realizado por Alhaddad [7] los resultados sobre el incremento en el reporte de correos maliciosos demuestrand, empleó un programa de entrenamiento de aprendizaje al momento, donde los usuarios víctimas de phishing eran redirigidos a una página de entrenamiento en lugar de un sitio malicioso; el estudio sostiene que, los usuarios son menos susceptibles a ser víctimas de phishing si recibieron este entrenamiento; la investigación realizada en este trabajo valida la conclusión del estudio, ya que los resultados sobre el incremento en el reporte de correos maliciosos demuestra cierto nivel de efectividad del aprendizaje al momento. Ahora bien, en cuanto al perfil de los usuarios, el estudio de Alhaddad

et al., determinó que el conocimiento en áreas de TI no garantiza estar a salvo de estas incidencias, por lo que el estudio precisa que el programa de formación es necesario para todos los perfiles de usuario.

Aunque plataformas como Microsoft 365 proporcionan un filtrado técnico eficaz, los resultados ponen sobre la mesa que ciertos vectores de ataque consiguen atravesar dicha barrera. Los resultados de este trabajo de titulación permiten demostrar que cuando la tecnología deja pasar amenazas, las estrategias de mitigación bien enfocadas al comportamiento del usuario actúan como una segunda línea de defensa que reduce el impacto de dichas filtraciones, sin embargo, no se puede afirmar que los resultados del trabajo se puedan extrapolar al resto de la institución puesto que el tamaño de la muestra sugiere una tendencia, pero se necesitaría una mayor cantidad de sujetos de estudio para elaborar una generalización sólida.

El trabajo de Hadnagy [33], en su libro sobre ingeniería social propone el concepto del "Firewall humano" que consiste en la capacidad de los miembros de una organización para resistir ataques de ingeniería social; en su trabajo, propone que este "Firewall" se puede fortalecer mediante entrenamiento basado en simulacros, con la finalidad de que el personal reconozca e identifique los ataques. Lo formulado por Hadnagy, se alinea con los resultados del trabajo de Brooks y McAndrew [5], Jibowu [34] y Alhaddad et al. [7], donde todos concluyen que la capacitación y concientización mediante escenarios reales aumenta el nivel de protección de los usuarios, y se refuerza aún más con los resultados del presente trabajo de investigación, ya que, mediante una simulación y una capacitación inmediata, se logró incrementar, aunque de forma parcial, la eficacia de la protección de datos en el sistema de correo electrónico institucional.

Kevin Mitnick en su libro sobre ingeniería social [10] detalla una serie de políticas que buscan reducir la incidencia de ataques de ingeniería social dentro de una organización; por otro lado, Hadnagy [33] se enfoca en la formación constante para fortalecer el "Firewall humano"; estas dos corrientes de acción conformaron el punto de partida para la elaboración de las políticas propuestas en este trabajo. Los principios de Mitnick sobre la debilidad del humano ante manipulación y comportamiento de manada sirven para definir los puntos débiles donde los ataques de ingeniería social tienen mayor incidencia, lo que a su vez corresponde con lo encontrado por Morić et al. [6], que establece la necesidad de desarrollar estrategias de entrenamiento sólidas ante la amenaza de la ingeniería social.

En comparación con los enfoques tradicionales, las políticas de seguridad tradicionales en las universidades suelen basarse en medidas estrictas. Esta investigación demuestra que el refuerzo positivo a través de la formación y los mecanismos de notificación simplificados produce un mejor cumplimiento que las políticas basadas en el miedo, lo que contradice los modelos de seguridad autoritarios más antiguos. Estos resultados se alinean con lo estipulado por [34], que concluye que el entrenamiento basado en escenarios y las simulaciones de phishing son importantes para reducir la incidencia de amenazas ocasionadas por los usuarios.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## 5.1 Conclusiones

- Este trabajo de titulación alcanzó su objetivo general a través del análisis de las técnicas de ingeniería social que atentan contra la infraestructura de correo electrónico institucional de la UNACH, y el desarrollo de estrategias de mitigación integran programas de sensibilización de los usuarios con políticas que formalizan protocolos de notificación y procedimientos de respuesta a incidentes, creando así una capa de defensa tanto para los datos personales como para los corporativos; y al alinear estas estrategias con las funciones básicas del NIST CFS, el estudio garantiza que los controles centrados en las personas sean más un complemento en lugar de sustituir las medidas de seguridad técnicas.
- Se identificaron y analizaron las técnicas de ingeniería social dirigidas a los sistemas de correo electrónico institucionales de la UNACH: phishing, el pretexting, el spear phishing, el baiting, el spoofing, el scareware y el typosquatting. Todas explotan vulnerabilidades técnicas y humanas. El phishing y el pretexting se perfilan como los vectores más extendidos debido a su escalabilidad y a que se basan en la confianza institucional, mientras que el spear phishing y el typosquatting ponen en peligro a figuras ejecutivas y administrativas con acceso a datos confidenciales. El análisis demuestra que la superficie de ataque de la UNACH se ve en peligro por la falta de concienciación sobre seguridad de los usuarios y desconocimiento de canales de denuncia.
- Se diseñaron estrategias no invasivas para la mitigación y prevención ante incidencias de ingeniería social con el fin de fortalecer la seguridad de los datos en los sistemas de correo electrónico de la UNACH que corresponden a políticas de manejo, formación, uso del sistema de correos, manejo de información sensible y acciones, y manejo de incidencias de ingeniería social; y a partir de las políticas, se generaron estrategias de manejo de incidencias de ingeniería social que consisten en propuestas de creación de un canal de reportes, clasificación de remitentes según incidencia de ataques, clasificación de correos mediante un perfilado de patrones de ataques y protocolos de acción correctivos. Las políticas y estrategias quedaron como propuesta debido a limitaciones administrativas en el proceso de modificación de políticas internas.
- Se evaluó la efectividad de las técnicas de ingeniería social y estrategias de mitigación mediante la aplicación del cuasiexperimento y se concluye que las estrategias de mitigación fueron parcialmente efectivas a la hora de proteger datos personales y corporativos debido a que los resultados indicaron que las estrategias basadas en el NIST CSF refuerzan significativamente la función DETECTAR, tal y como se demostró con la notable mejora del grupo experimental a la hora de notificar correos electrónicos sospechosos como indica el valor-p de la prueba de McNemar ($p=0.0026$), indicando un cambio estadísticamente significativo; sin embargo, estas estrategias resultaron estadísticamente ineficientes a la hora de reducir los comportamientos de riesgo de carácter pasivo en el grupo de control, entre los que figuran hacer clic en enlaces ($p=0.07$), abrir correos electrónicos ($p=0.61$) y facilitar credenciales ($p=1.00$), indicando cambios no significativos.

## 5.2 Recomendaciones

- Para futuras pruebas de phishing, se recomienda utilizar una muestra de la población universitaria más grande y variada que en lo posible abarque miembros de todas las facultades, cargos y semestres posibles, diversificando los individuos de la muestra para obtener una mejor representación de toda la comunidad universitaria.
- Se recomienda realizar un seguimiento al estado de los datos personales del personal institucional, ya que al pertenecer a un cargo importante son más propensos a que su información se divulgue o ya se encuentre en línea. Además, se debe indagar cómo los modelos de lenguaje generativo pueden ser usados para redactar mensajes personalizados de forma masiva. Y en función de ambos puntos, tomar medidas de prevención para mitigar casos de Spear Phishing dirigidos a miembros de alto perfil de la comunidad universitaria.
- Para concientizar a la comunidad universitaria de cómo proceder ante un ataque de ingeniería social, se recomienda realizar campañas de concientización más allá del correo electrónico. Estas campañas se deberán realizar para todos los miembros de la comunidad universitaria de forma periódica; para las campañas, se recomienda el uso de programas de entrenamiento al momento ya que estudios demuestran que este tipo de programas de formación ayudan a disminuir la incidencia de ataques de ingeniería social; adicionalmente, se recomienda una campaña de gran alcance una vez por año para todos los miembros de la comunidad universitaria, ya que actualmente solo se realizan capacitaciones para miembros directivos, docentes y empleados dejando de lado a los estudiantes.
- Para la plataforma institucional, se recomienda implementar una solución de detección de fraude a nivel de la infraestructura institucional; ya que, si los ataques de ingeniería social se mantienen en aumento, las estrategias no invasivas dejarían de ser suficientes para prevenir y mitigar los riesgos.

# BIBLIOGRAFÍA


[1] M. A. Siddiqi, W. Pak, y M. A. Siddiqi, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures", *Appl. Sci.*, vol. 12, núm. 12, p. 6042, jun. 2022, doi: 10.3390/app12126042.

[2] C. D. Hylender, P. Langlois, A. Pinto, y S. Widup, "Data Breach Investigations Report (DBIR)", 2024. Consultado: el 26 de marzo de 2026. [En línea]. Disponible en: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[3] Universidad Nacional de Chimborazo, "Política de protección de datos personales", UNACH. Consultado: el 15 de abril de 2026. [En línea]. Disponible en: https://www.unach.edu.ec/politica-de-proteccion-de-datos-personales/

[4] K. Althobaiti y N. Alsufyani, "A review of organization-oriented phishing research", *PeerJ Comput. Sci.*, vol. 10, p. e2487, nov. 2024, doi: 10.7717/peerj-cs.2487.

[5] D. A. Brooks y I. R. McAndrew, "Cyber Threat Intelligence Driven Phishing Awareness Programs: A Qualitative Exploratory Study", United States -- Maryland, 2023. [En línea]. Disponible en: https://www.proquest.com/dissertations-theses/cyber-threat-intelligence-driven-phishing/docview/2832622897/se-2?accountid=36757

[6] Z. Morić, V. Dakić, M. Plećaš, y I. Ogrizek Biškupić, "Evaluating End-User Defensive Approaches Against Phishing Using Education and Simulated Attacks in a Croatian University", *Journal of Cybersecurity and Privacy*, vol. 5, núm. 3, p. 38, jun. 2025, doi: 10.3390/jcp5030038.

[7] M. Alhaddad, M. Mohd, F. Qamar, y M. Imam, "Study of Student Personality Trait on Spear-Phishing Susceptibility Behavior", *International Journal of Advanced Computer Science and Applications*, vol. 14, núm. 5, pp. 667–678, 2023, doi: 10.14569/IJACSA.2023.0140571.

[8] M. Schmitt y I. Flechais, "Digital deception: generative artificial intelligence in social engineering and phishing", *Artif. Intell. Rev.*, vol. 57, núm. 12, dic. 2024, doi: 10.1007/s10462-024-10973-2.

[9] K. Khadka, A. B. Ullah, W. Ma, E. M. Marroquin, y Y. Alem, "A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing", *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1631–1638, nov. 2023, doi: 10.1109/TrustCom60117.2023.00222.

[10] K. D. Mitnick y W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc., 2002.

[11] W. Han, J. Zhu, C. Zhang, Z. Zhang, Y. Mei, y L. Wang, "Phish-Master: Leveraging Large Language Models for Advanced Phishing Email Generation and Detection", *Appl. Sci.*, vol. 15, núm. 22, nov. 2025, doi: 10.3390/app152212203.

[12] P. Dewan, A. Kashyap, y P. Kumaraguru, "Analyzing Social and Stylometric Features to Identify Spear phishing Emails", *APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–13, jun. 2014, Consultado: el 6 de marzo de 2026. [En línea]. Disponible en: http://arxiv.org/abs/1406.3692

[13] J. Osamor, M. Ashawa, A. Shahrabi, A. Philip, y C. Iwendi, "The Evolution of Phishing and Future Directions: A Review", *International Conference on Cyber Warfare and Security*, vol. 20, núm. 1, pp. 361–368, mar. 2025, doi: 10.34190/iccws.20.1.3366.

[14] R. Dilworth, "StegoStylo: Squelching Stylometric Scrutiny through Steganographic Stitching", ene. 2026, Consultado: el 14 de abril de 2026. [En línea]. Disponible en: https://arxiv.org/pdf/2601.09056v2

[15] G. Sachdev, "Ranking Social Engineering Attack Vectors in The Healthcare and Public Health Sector", Tesis de Maestría, Purdue University, 2023. doi: 10.25394/PGS.22006688.V1.

[16] N. Ukwadinachi, "From Mitnick to Modern Database Threats: Evolution of Social Engineering Tactics and Their Impact on Data Integrity", *Journal of Technology Studies*, vol. 50, núm. 1, pp. 14–29, jul. 2025, doi: 10.21061/jts.438.

[17] J. R. Whiteman III, "Social Engineering: Humans are the Prominent Reason for the Continuance of These Types of Attacks", United States -- New York, 2017. [En línea]. Disponible en: https://www.proquest.com/dissertations-theses/social-engneering-humans-are-prominent-reason/docview/2007620740/se-2?accountid=36757

[18] T. Longtchi, R. M. Rodriguez, L. Al-Shawaf, A. Atyabi, y S. Xu, "Internet-based Social Engineering Attacks, Defenses and Psychology: A Survey", *arXiv preprint arXiv:2203.08302*, pp. 1–30, ago. 2022, Consultado: el 6 de marzo de 2026. [En línea]. Disponible en: http://arxiv.org/abs/2203.08302

[19] P. Ramesh, D. L. Bhaskari, y CH. Satyanarayana, "A Comprehensive Analysis of Spoofing", *International Journal of Advanced Computer Science and Applications*, vol. 1, núm. 6, 2010, doi: 10.14569/ijacsa.2010.010623.

[20] Y. Aun, M. L. Gan, N. H. B. A. Wahab, y G. H. Guan, “Social Engineering Attack Classifications on Social Media Using Deep Learning”, *Computers, Materials and Continua*, vol. 74, núm. 3, pp. 4917–4931, 2023, doi: 10.32604/cmc.2023.032373.

[21] M. Muzammil, Z. Wu, L. Harisha, B. Kondracki, y N. Nikiforakis, “Typosquatting 3.0: Characterizing Squatting in Blockchain Naming Systems”, *APWG Symposium on Electronic Crime Research (eCrime)*, pp. 94–108, nov. 2024, Consultado: el 12 de marzo de 2026. [En línea]. Disponible en: http://arxiv.org/abs/2411.00352

[22] C. Abásolo, “«rnicrosoft», la estafa del cambio de letras de los hackers para hacerse pasar por Microsoft”, *softzone*, el 4 de diciembre de 2025. Consultado: el 13 de mayo de 2026. [En línea]. Disponible en: https://www.softzone.es/noticias/seguridad/rnicrosoft-estafa-typosquatting-hackers/

[23] C. Pascoe, S. Quinn, y K. Scarfone, “Spanish Translation of the NIST Cybersecurity Framework 2.0”, 2024, doi: 10.6028/NIST.CSWP.29.spa.

[24] Asamblea Nacional de la República del Ecuador, “Constitución de la República del Ecuador”, *Registro Oficial*, vol. 449, núm. 20, 2008, Consultado: el 12 de marzo de 2026. [En línea]. Disponible en: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

[25] A. Camacho Coronel, J. M. Erazo Ayón, C. Salazar Tovar, y B. Pardo Centanaro, “Ingeniería Social: Revisión Sistemática de Phishing y Pretexting en Plataformas Académicas”, *RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação*, núm. 72, pp. 122–136, 2024, Consultado: el 12 de marzo de 2026. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9852055&info=resumen&idioma=SPA

[26] R. Hernández Sampieri, C. F. Fernandez-Collado, y P. Baptista Lucio, *Metodología de la investigación*, 6a ed. México D.F.: McGraw-Hill Education, 2014.

[27] D. C. Montgomery, G. C. Runger, y trad. R. Piña, *Probabilidad y estadística aplicadas a la ingeniería*. Limusa Wiley, 2013.

[28] B. Vidakovic, *Engineering Biostatistics*. John Wiley & Sons, 2017.

[29] IEEE, *ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes -- Risk management*. New York, NY, USA., 2021.

[30] L. de Salvador, “Ingeniería Social y Operaciones Psicológicas en Internet”, Madrid, 2011. Consultado: el 5 de abril de 2026. [En línea]. Disponible en:

https://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

[31] C. R. Kothari, *Research methodology : methods & techniques*. New Age International (P) Ltd., 2004.

[32] J. W. Creswell, *Qualitative inquiry & research design : choosing among five approaches*. Sage Publications, 2007.

[33] C. Hadnagy, *Social engineering : the science of human hacking*. John Wiley & Sons, Inc., 2018.

[34] D. O. Jibowu, "Information Technology Managers' Strategies for Securing Organizational Networks From Cyberattacks", United States -- Minnesota, 2025. [En línea]. Disponible en: https://www.proquest.com/dissertations-theses/information-technology-managers-strategies/docview/3288153818/se-2?accountid=36757

[35] ISO/IEC [organización], "Information technology — Security techniques — Information security management systems — Overview and vocabulary", Geneva, 2018.

[36] NIST, "Access", 2024. [En línea]. Disponible en: https://csrc.nist.gov/glossary

[37] M. Ahmed, A. N. Mahmood, y J. Hu, "A survey of network anomaly detection techniques", *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[38] D. C. Plummer, "An Ethernet Address Resolution Protocol", nov. 1982.

[39] ISO/IEC, "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements", 2022, *Geneva, Switzerland*.

[40] NIST, "Digital Identity Guidelines: Authentication and Lifecycle Management", 2017.

[41] R. Sandhu y P. Samarati, "Access control: principle and practice", *IEEE Communications Magazine*, vol. 32, núm. 9, pp. 40–48, sep. 1994.

[42] M. Conti, T. Dargahi, y A. Dehghantanha, *Cyber Threat Intelligence: Challenges and Opportunities*. Springer, 2018.

[43] P. G. Neumann, *Computer-Related Risks*. Addison-Wesley, 1995.

[44] A. S. Tanenbaum, *Modern Operating Systems*, 4a ed. Boston, MA, USA: Pearson, 2014.

[45] ISO/IEC, “ISO/IEC 27000:2022 Information technology — Security techniques — Information security management systems — Overview and vocabulary”, 2022, *Geneva, Switzerland*.

[46] NIST, “Digital Identity Guidelines”, 2017.

[47] R. Heartfield y G. Loukas, “A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks”, *ACM Comput. Surv.*, vol. 48, núm. 3, pp. 1–39, feb. 2016.

[48] Verizon, “2024 Data Breach Investigations Report”, 2024.

[49] D. Loshin, *Enterprise Knowledge Management: The Data Quality Approach*. Morgan Kaufmann, 2001.

[50] NIST, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”, 2020.

[51] European Parliament, *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. 2016. Consultado: el 14 de mayo de 2026. [En línea]. Disponible en: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[52] A. K. Pillai, “Spotting the Deepfake”, julio de 2024. [En línea]. Disponible en: https://transmitter.ieee.org

[53] NIST, “An Introduction to Information Security”, 2017.

[54] P. Mockapetris, “Domain names - concepts and facilities”, Internet Engineering Task Force, RFC 1034.

[55] D. Crocker, T. Hansen, y M. Kucherawy, “DomainKeys Identified Mail (DKIM) Signatures”, Internet Engineering Task Force, RFC 6376.

[56] M. Kucherawy y E. Zwicky, “Domain-based Message Authentication, Reporting, and Conformance (DMARC)”, mar. 2015.

[57] P. Resnick, “Internet Message Format”, Internet Engineering Task Force, RFC 5322.

[58] P. Juola, “Authorship Attribution”, *Foundations and Trends in Information Retrieval*, vol. 1, núm. 3, pp. 233–334, 2006.

[59] NIST, “Guide for Conducting Risk Assessments”, 2012.

[60] C. Miller y others, *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Addison-Wesley Professional, 2006.

[61] NIST, “Glossary of Key Information Security Terms”, 2023.

[62] NIST, “Building an Information Technology Security Awareness and Training Program”, 2023.

[63] A. T. S. A. Alhaj y S. M. H. B. Zain, “Financial Fraud Detection Using Machine Learning Techniques: A Review”, *IEEE Access*, vol. 11, pp. 23456–23478, 2023.

[64] D. M. Kroenke y D. J. Auer, *Database Concepts*, 8a ed. Pearson, 2017.

[65] ISO/IEC, “ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance”, 2017, *Geneva, Switzerland*.

[66] S. Gibson, *Hacking: The Art of Exploitation*, 2nd ed. No Starch Press, 2008.

[67] S. M. Martínez Monterrubio, J. Frausto Solis, y J. A. Recio García, “THREATMOSAIC: collection, curation and enrichment of indicators of compromise (IOCs)”, *International Journal of Combinatorial Optimization Problems and Informatics*, vol. 16, núm. 3, pp. 441–457, jul. 2025, doi: 10.61467/2007.1558.2025.v16i3.848.

[68] NIST, “Risk Management Framework for Information Systems and Organizations”, 2018.

[69] CISA, “Critical Infrastructure Sectors”, 2024. [En línea]. Disponible en: https://www.cisa.gov

[70] K. Mitnick y W. Simon, *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.

[71] NIST, “Glossary of Key Information Security Terms”, 2023.

[72] T. B. Brown *et al.*, “Language Models are Few-Shot Learners”, *Adv. Neural Inf. Process. Syst.*, vol. 33, pp. 1877–1901, 2020.

[73] E. Skoudis y L. Zeltser, *Malware: Fighting Malicious Code*. Prentice Hall PTR, 2004.

[74] N. Borisov, I. Goldberg, y D. Wagner, “Intercepting mobile communications: the insecurity of 802.11”, en *Proc. 7th Annual International Conference on Mobile Computing and Networking*, 2001, pp. 180–189.

[75] A. L. Young y M. Yung, “Cryptovirology: Extortion-Based Security Threats and Countermeasures”, en *IEEE Symposium on Security and Privacy*, 1996, pp. 129–140.

[76] J. Klensin, “Simple Mail Transfer Protocol”, Internet Engineering Task Force, RFC 5321.

[77] K. Mitnick y W. Simon, *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.

[78] T. Berners-Lee, R. Fielding, y L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax”, Internet Engineering Task Force, RFC 3986.

[79] MITRE Corporation, “Common Vulnerabilities and Exposures (CVE)”, 2024. [En línea]. Disponible en: https://cve.mitre.org

[80] J. J. T. Wang y others, “Vishing: A New Voice Phishing Attack”, *IEEE Trans. Dependable Secure Comput.*, vol. 18, núm. 4, pp. 1567–1581, jul. 2021.

## ANEXOS

**Anexo 1:** Glosario de Términos.

**A**

**Activo estratégico:** Recursos crítico que una organización debe protege. Incluye datos, sistemas, infraestructura, personal. Son necesarios para cumplir objetivos empresariales y mantener operaciones en marcha [35].

**Acceso:** La capacidad de alguien para interactuar con datos, recursos o sistemas. Generalmente está controlada mediante autenticación y autorización [36].

**Anomalía:** Comportamiento o patrón inusual en datos o sistemas. Puede indicar un error técnico o una amenaza de seguridad [37].

**ARP (Address Resolution Protocol):** Protocolo de red definido en RFC 826 que mapea direcciones IP a direcciones MAC en redes IPv4, operando en la capa de enlace de datos del modelo OSI [38].

**Auditorías Regulares:** Exámenes periódicos documentados de los controles de seguridad, políticas y procedimientos de una organización. Su objetivo es verificar el cumplimiento de estándares como ISO 27001 [39].

**Autenticación Multifactorial (MFA):** Sistema que requiere más de un factor para acceder. Por ejemplo: contraseña más código de teléfono. Es mucho más seguro que solo una contraseña [40].

**Autoridad:** Un rol que tiene derechos para tomar decisiones, otorgar permisos o aplicar controles de seguridad dentro de una organización [41].

**B**

**Baiting:** El atacante pone algo tentador al alcance de la víctima, una descarga gratuita, un USB olvidado y esperar. La curiosidad hace el resto [42].

**Brechas de Seguridad:** Incidentes donde se produce acceso no autorizado a sistemas, aplicaciones, resultando en divulgación, alteración o destrucción no autorizada de información [43].

**Bot:** Aféresis de robot, es un programa informático que efectúa tareas automáticas y reiterativas mediante Internet a través de una cadena de comandos o funciones autónomas previas [44].

**C**

**Ciberseguridad:** Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, extendiéndose a propiedades como autenticidad, responsabilidad, no repudio y confiabilidad [45].

**Credenciales:** Lo que le prueba al sistema quién eres. Casi siempre es una combinación de algo que te identifica y algo que confirma que eres tú. Los sistemas de autenticación viven de eso [46].

**Cebo:** Lo que el atacante pone al alcance de la víctima y lo tome sin pensar. La apuesta es que la curiosidad gane antes que el sentido común. [42].

**Clone Phishing:** Tipo de ataque de phishing donde el atacante replica un correo electrónico legítimo previamente entregado, modificando enlaces o archivos adjuntos maliciosos para explotar la confianza existente [47].

**Componentes Humano:** Factor humano en ciberseguridad que refiere a situaciones donde el error humano (negligencia, falta de conocimiento, acciones maliciosas internas) resulta en brecas de seguridad exitosas [48].

**D**

**Datos Corporativos:** Información de una organización en el curso de sus operaciones comerciales que incluye datos financieros, operativos, estratégicos y de recursos humanos [49].

**Datos Sensibles:** Información que si llega a ser difundida o manipulada podría causar daño significativo a individuos u organizaciones [50].

**Datos Personales:** Cualquier información que lleve a una persona real. Nombre, correo, número de teléfono, incluso la dirección IP. Si con eso se puede identificar a alguien, cuenta. Regulaciones como el GDPR existen precisamente para controlar quién puede recopilar esa información. [51].

**Deepfake:** Contenido sintético mediante inteligencia artificial (aprendizaje profundo) que representa a personales reales acciones o declaraciones que no ocurrieron, representando amenazas y pasa para la desinformación y fraude [52].

**Diseño de Políticas:** Poner en escrito cómo se protege lo que importa. Quién tiene acceso a qué sistemas, qué se hace si hay una brecha, quién responde ante un incidente. Es lo que evita que cada empleado tome decisiones de seguridad por su cuenta [53].

**DNS (Domain Name System):** Sistema de nombres de dominio que traduce nombres legibles por humanos a direcciones IP [54].

**DKIM (DomainKeys Identified Mail):** Protocolo de autenticación de correo electrónico definido en RFC 6376 que utiliza criptografía de clave pública para firmar mensajes y verificar autenticidades de dominios [55].

**DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Protocolo especificado en RFC 7489 que utiliza resultados de SPF y DKIM para autenticar mensajes y proporcionar políticas de manejo de fallos y reportes [56].

## E

**Email Header:** Lo que viaja antes del mensaje y que casi nadie lee. Contiene los metadatos del correo. Los sistemas de autenticación y los filtros de spam dependen de esa información para decidir si el correo es legítimo [57].

**Estilometría:** Analizar cómo escribe alguien para descubrir quién escribió algo. Longitud de oraciones, vocabulario recurrente, patrones de puntuación. Cada persona deja una huella lingüística. Se usa en investigaciones forense digital y atribución de autoría. [58].

**Estrategias de Mitigación:** Lo que se implementa para reducir el impacto de un riesgo. Puede ser un control técnico, un procedimiento interno, o una política. [59].

**Explotación:** Cuando alguien no solo encuentra una vulnerabilidad, sino que la usa. Con el código o la técnica correcta, una falla en el sistema se convierte en acceso no autorizado, privilegios elevados, o control total. [60].

**Exposición:** El estado en que queda un sistema cuando algo no está bien configurado o le faltan controles básicos. No hace falta que alguien ataque, ya que la exposición ya es riesgo [61].

**F**

**Factor Humano:** La parte más impredecible de cualquier sistema. No es un problema de tecnología. Es un problema de comportamiento, y eso es mucho más difícil de resolver [48].

**Formación en Concienciación:** Programa fundamental de capacitación en ciberseguridad para todo el personal, diseñado para ayudar a comprender roles en la protección de activos y riesgos asociados [62].

**Fraudes Financieros:** Actividades ilegales y engañosas para obtener ganancia financiera, robo de identidad o fraude en pagos [63].

**G**

**Gestión de Datos:** Cómo una organización controla su información. Sin procesos claros, los datos se acumulan sin orden, duplicados, desactualizados, y nadie responde cuando algo sale mal [64].

**Guía:** Documento que explica cómo hacer algo concreto en seguridad. Más específico que una política, aquí no se define qué lograr, sino los pasos para lograrlo [65].

**H**

**Hacker:** Persona con conocimiento técnico profundo de sistemas informáticos. El término tiene mala fama que no siempre es justa, hay hackers que atacan sistemas ajenos y hackers contratados para encontrar fallas antes que los atacantes. Lo que los separa no es la habilidad sino para quién trabaja y con qué permiso [66].

## I

**Indicadores de Compromiso (IoC):** Las huellas que deja un ataque, a veces antes de que alguien lo note. Tráfico anómalo, configuraciones modificadas sin explicación, procesos corriendo donde no deberían. Ninguno solo es prueba definitiva, pero varios juntos son razón suficiente para levantar sospechas [67].

**Implementación:** El paso entre tener una política y que realmente funcione. Alguien tiene que desplegarla técnicamente, capacitar al equipo, asignar quién responde por qué, y verificar que lo que dice el documento ocurra en la práctica [68].

**Infraestructura Crítica:** Los sistemas cuya falla no afecta solo a una organización. Si se interrumpen, las consecuencias se sienten fuera de cualquier perímetro corporativo. Por eso son blancos frecuentes y por eso su protección está regulada de forma diferente [69].

**Ingeniería Social:** Conjunto de tácticas para manipulas, influenciar o engañar a víctimas para divulgar información sensible o realizar acciones contrarias a la seguridad, explotando la tendencia humana a confiar [70].

## L

**Lista Negra:** Lista de entidades como direcciones IP, dominios o correos electrónicos bloqueadas del acceso a sistemas [71].

**LLM (Large Language Model):** Modelo de inteligencia artificial entrenado en grandes cuerpos de texto que genera contenido mediante aprendizaje profundo y redes neuronales [72].

## M

**Malware:** Software diseñado para causar daño. Puede robar credenciales, cifrar archivos y exigir pago, propagarse por la red sin intervención humana, o instalarse en silencio y esperar. Los mecanismos varían, pero todos comparten el mismo punto de partida: código ejecutándose en un sistema sin que el dueño lo haya autorizado [73].

**MITM (Man-in-the-Middle):** Un atacante que se interpone entre dos partes que creen comunicarse directamente. Desde esa posición puede leer el tráfico, modificar mensajes en tránsito, o suplantar uno de los extremos. Lo más problemático no es el ataque en sí, es que puede ocurrir sin que ninguna de las partes lo note hasta que ya es tarde [74].

**R**

**Ransomware:** Tipo de malware que cifra datos o bloquea sistemas, exigiendo pago de rescate para restaurar el acceso, representando una de las amenazas más significativas para organizaciones [75].

**S**

**SMTP (Simple Mail Transfer Protocol):** Protocolo fundamental definido en RFC 5321 para transmisión de correo electrónico entre servidores, especificando comandos, códigos de respuesta y manejo de conexiones [76].

**T**

**Técnicas de Ingeniería Social:** Métodos específicos de manipulación psicológica incluyendo phishing, pretexting, baiting, vishing y tailgating, diseñados para engañar a usuarios y eludir controles técnicos [77].

**U**

**URL (Uniform Resource Locator):** Identificador estándar de recursos en el web definido en RFC 3986 que especifica la ubicación y mecanismos de acceso a recursos mediante sintaxis estructurada [78].

**V**

**Vulnerabilidad:** Debilidad de un sistema, software o componentes que puede ser explotada por amenazas para causar daño, catalogada en bases de datos como CVE (Common Vulnerabilities and Exposures) [79].

**Vishing:** Forma de phishing que utiliza llamadas telefónicas o comunicación de voz para engañar a víctimas y obtener información sensible empleando técnicas de ingeniería social y suplantación de identidad [80].

**Anexo 2:** Cuestionario para el personal general.

**Pregunta 1:** ¿Es capaz de identificar visualmente un correo de suplantación de identidad (Phishing)?

**Respuestas:**

1. Si
2. No
3. No estoy seguro

**Pregunta 2:** ¿Ha recibido correos que intentaban generar urgencia o miedo injustificado (ej. avisos de bloqueo de cuenta, amenazas) durante el último año?

**Respuestas:**

1. Sí, en múltiples ocasiones
2. Sí, en una ocasión
3. Tal vez, no estoy seguro
4. No, nunca

**Pregunta 3:** ¿Ha notado errores gramaticales o direcciones de remitente extrañas en correos que supuestamente son institucionales?

**Respuestas:**

1. Sí, frecuentemente
2. Ocasionalmente
3. Rara vez
4. Nunca

**Pregunta 4:** ¿Conoce la política institucional sobre el manejo de datos confidenciales en el correo electrónico?

**Respuestas:**

1. Sí, la conozco a fondo
2. Tengo conocimientos generales
3. He oído hablar de ella, pero no la conozco
4. No

**Pregunta 5:** ¿Sabe cuál es el canal oficial para reportar un correo sospechoso en la UNACH?

**Respuestas:**

1. Sí, lo sé y lo he usado
2. Sí, lo sé, pero no lo he usado
3. No estoy seguro
4. No lo sé

**Pregunta 6:** ¿Ha participado en charlas o capacitaciones sobre seguridad de la información recientemente?

**Respuestas:**

1. Sí, en el último año
2. Sí, hace más de un año
3. No recuerdo
4. No, nunca

**Pregunta 7:** ¿Considera que sus credenciales de correo (usuario y contraseña) son activos críticos que deben ser protegidos para evitar robo de información?

**Respuestas:**

1. Totalmente de acuerdo
2. De acuerdo
3. En desacuerdo
4. Totalmente en desacuerdo

**Pregunta 8:** Si recibe un correo aparentemente de una autoridad solicitando con urgencia datos confidenciales o transferencias ¿Qué acción debería tomar según las políticas de seguridad?

**Respuestas:**

1. Verificar la solicitud por un canal alternativo (llamada telefónica o presencial) antes de realizar cualquier acción
2. Responder inmediatamente al correo para no hacer esperar a la autoridad
3. Reenviar el correo a un compañero para pedir su opinión
4. Ignorar el correo sin reportarlo a nadie

**Pregunta 9:** Ante un archivo adjunto inesperado de un contacto conocido ¿Qué acción toma primero?

**Respuestas:**

1. Confirmar con el remitente que envió el archivo antes de descargar
2. Descargarlo y abrirlo para ver el contenido
3. Escanearlo con el antivirus de mi PC
4. Eliminarlo de inmediato

**Anexo 3:** Cuestionario para el personal técnico

**Pregunta 1:** ¿Con qué frecuencia identifica intentos de Spear Phishing (ataques dirigidos) hacia la alta dirección o usuarios críticos?

**Respuestas:**

1. Múltiples ocasiones al día
2. Varias veces a la semana
3. Ocasionalmente
4. Nunca / No estoy seguro

**Pregunta 2:** ¿Utiliza herramientas de análisis de encabezados de correo para validar la legitimidad del mensaje?

**Respuestas:**

1. Siempre, como parte del protocolo
2. A veces
3. Rara vez
4. Nunca, solo confío en el filtro automático

**Pregunta 3:** ¿Ha detectado dominios spoofeados (tipográficamente engañosos, ej. @unnach.com en lugar de @unach.edu.ec) apuntando a la institución?

**Respuestas:**

1. Múltiples ocasiones
2. Una ocasión
3. No estoy seguro
4. Nunca

**Pregunta 4:** ¿Se aplican filtros de correo (SPAM/Virus) alineados con el marco de seguridad NIST en el servidor institucional?

**Respuestas:**

1. Sí
2. No

**Pregunta 5:** ¿Existe un procedimiento documentado y activo para la respuesta a incidentes de seguridad vía correo?

**Respuestas:**

1. Sí, un plan formalizado
2. Existen instrucciones informales
3. Se actúa según criterio del técnico de turno
4. No existe procedimiento

**Pregunta 6:** ¿Considera que la autenticación multifactorial (MFA) está implementada eficazmente para mitigar el robo de credenciales en el correo?

**Respuestas:**

1. Sí, es obligatoria y robusta
2. Sí, pero tiene fallos o excepciones
3. Está implementada parcialmente
4. No está implementada

**Pregunta 7:** ¿Cuál es el tiempo promedio de respuesta para aislar un buzón comprometido tras una alerta confirmada de phishing?

**Respuestas:**

1. Inmediatamente (Automático o < 15 minutos)
2. Menos de 1 hora
3. Durante el transcurso del día
4. Más de 24 horas

**Pregunta 8:** Ante una campaña masiva de ingeniería social (ej. Phishing masivo) ¿Cuál es la primera acción técnica que debe priorizar el área de TI?

**Respuestas:**

1. Activar los protocolos de respuesta a incidentes y bloquear el remitente/dominio en los filtros de correo
2. Informar únicamente a los usuarios para que eliminen el correo manualmente
3. Revisar los logs del servidor después de que termine el incidente
4. Esperar a recibir quejas de usuarios para confirmar la gravedad

**Pregunta 9:** ¿Conoce si se realizan campañas de concientización o pruebas de penetración (Simulaciones de Phishing) a los usuarios para medir su resistencia?

**Respuestas:**

1. Sí, de forma periódica y programada
2. Sí, pero esporádicamente
3. Se ha hecho alguna vez
4. Nunca se han realizado

**Anexo 4:** Respuestas del cuestionario para el personal general.

Las tablas 16 y 17 contienen las respuestas de los cuestionarios para el personal general.

**Tabla 16:** Respuestas del cuestionario para el personal general.

| Pregunta | Respuesta 1 | Respuesta 2 | Respuesta 3 | Respuesta 4 |
|---|---|---|---|---|
| ¿Es capaz de identificar visualmente un correo de suplantación de identidad (Phishing) | 8 | 2 | 0 | 0 |
| ¿Ha recibido correos que intentaban generar urgencia o miedo injustificado (ej. avisos de bloqueo de cuenta, amenazas) durante el último año? | 0 | 7 | 2 | 1 |
| ¿Ha notado errores gramaticales o direcciones de remitente extrañas en correos que supuestamente son institucionales? | 0 | 3 | 4 | 3 |
| ¿Conoce la política institucional sobre el manejo de datos confidenciales en el correo electrónico? | 0 | 0 | 2 | 8 |
| ¿Sabe cuál es el canal oficial para reportar un correo sospechoso en la UNACH? | 0 | 0 | 3 | 7 |
| ¿Ha participado en charlas o capacitaciones sobre seguridad de la información recientemente? | 0 | 0 | 2 | 8 |
| ¿Considera que sus credenciales de correo (usuario y contraseña) son activos críticos que deben ser protegidos para evitar robo de información? | 10 | 0 | 0 | 0 |
| Si recibe un correo aparentemente del Rector o una autoridad, solicitando con urgencia datos confidenciales o transferencias, ¿qué acción debería tomar según las políticas de seguridad? | 8 | 2 | 0 | 0 |
| Ante un archivo adjunto inesperado de un contacto conocido, ¿Qué acción toma primero? | 6 | 0 | 3 | 1 |

**Anexo 5:** Respuestas del cuestionario para el personal técnico.

**Tabla 17:** Respuestas del cuestionario para el personal técnico.

| Pregunta | Respuesta 1 | Respuesta 2 | Respuesta 3 | Respuesta 4 |
|---|---|---|---|---|
| ¿Es capaz de identificar visualmente un correo de suplantación de identidad (Phishing) | 6 | 3 | 1 | 0 |
| ¿Ha recibido correos que intentaban generar urgencia o miedo injustificado (ej. avisos de bloqueo de cuenta, amenazas) durante el último año? | 0 | 0 | 3 | 7 |
| ¿Ha notado errores gramaticales o direcciones de remitente extrañas en correos que supuestamente son institucionales? | 3 | 4 | 3 | 0 |
| ¿Conoce la política institucional sobre el manejo de datos confidenciales en el correo electrónico? | 9 | 1 | 0 | 0 |

| | | | | |
|---|---|---|---|---|
| ¿Sabe cuál es el canal oficial para reportar un correo sospechoso en la UNACH? | 0 | 2 | 5 | 3 |
| ¿Ha participado en charlas o capacitaciones sobre seguridad de la información recientemente? | 7 | 3 | 0 | 0 |
| ¿Considera que sus credenciales de correo (usuario y contraseña) son activos críticos que deben ser protegidos para evitar robo de información? | 0 | 4 | 6 | 0 |
| Si recibe un correo aparentemente del Rector o una autoridad, solicitando con urgencia datos confidenciales o transferencias, ¿qué acción debería tomar según las políticas de seguridad? | 6 | 2 | 2 | 0 |
| Ante un archivo adjunto inesperado de un contacto conocido, ¿Qué acción toma primero? | 0 | 0 | 0 | 10 |

**Anexo 6:** Videos correspondientes a la capacitación.

https://drive.google.com/drive/folders/1fuHio5MhcjeZEBnxMhCAVv730dzv04MT

**Anexo 7:** Datos del Pretest.

## Grupo A

Las tablas 18 y 19 contienen los datos sobre el Pretest de cada grupo respectivamente.

**Tabla 18:** Datos de la simulación Pretest grupo A.

| Grupo A | Plantilla | Fecha Envío | Estado | ABIERTO | ENLACE_ CLICADO | DATOS_ ENVIADOS | REPORTADO |
|---|---|---|---|---|---|---|---|
| Estudiante 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Estudiante 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Estudiante 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 0 |
| Estudiante 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 1 | 0 |
| Estudiante 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Empleado 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Empleado 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Empleado 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Empleado 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 1 | 0 |
| Empleado 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Directivo 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |

## Grupo B

**Tabla 19:** Datos de la simulación Pretest grupo B.

| Grupo B | Plantilla | Fecha Envío | Estado | ABIERTO | ENLACE_ CLICADO | DATOS_ ENVIADOS | REPORTADO |
|---|---|---|---|---|---|---|---|
| Estudiante 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 1 | 0 |
| Estudiante 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Estudiante 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Estudiante 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 0 |
| Estudiante 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Empleado 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 0 |
| Empleado 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Empleado 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Empleado 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Empleado 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Directivo 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Directivo 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 1 | 0 |
| Directivo 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |

**Anexo 8:** Datos del Postest.

## Grupo A

Las tablas 20 y 21 contienen los datos sobre el Pretest de cada grupo respectivamente.

**Tabla 20:** Datos de la simulación Postest grupo A.

| Grupo A | Plantilla | Fecha Envío | Estado | ABIERTO | ENLACE_ CLICADO | DATOS_ ENVIADOS | REPORTADO |
|---|---|---|---|---|---|---|---|
| Estudiante 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Estudiante 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 0 |
| Estudiante 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Estudiante 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Estudiante 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Empleado 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Empleado 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Empleado 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Empleado 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Empleado 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Directivo 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Directivo 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Directivo 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 0 |
| Directivo 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Directivo 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |

## Grupo B

**Tabla 21:** Datos de la simulación Postest grupo B.

| Grupo B | Plantilla | Fecha Envío | Estado | ABIERTO | ENLACE_ CLICADO | DATOS_ ENVIADOS | REPORTADO |
|---|---|---|---|---|---|---|---|
| Estudiante 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 1 | 1 |
| Estudiante 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Estudiante 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |
| Estudiante 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Estudiante 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 1 |
| Empleado 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 0 |
| Empleado 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Empleado 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Empleado 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 1 |
| Empleado 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 1 | 0 | 1 |
| Directivo 1 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |
| Directivo 2 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Directivo 3 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 1 |
| Directivo 4 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 0 | 0 | 0 | 1 |
| Directivo 5 | Problemas de cobro en Google Services - Gemini | 26/01/2026 | Enviado | 1 | 0 | 0 | 1 |

**Anexo 9:** Tablas de contingencia

Las tablas de la 22, 23, 24 y 25 contienen las matrices de contingencia para cada variable en el Pretest respectivamente.

**Tabla 22:** Matriz de contingencia para la variable CLIC del grupo A.

| Clic | 0 | 1 | total |
|---|---|---|---|
| **0** | 4 | 2 | 6 |
| **1** | 7 | 2 | 9 |
| **total** | 11 | 4 | |

**Tabla 23:** Matriz de contingencia para la variable ABIERTO del grupo A.

| Abierto | 0 | 1 | total |
|---|---|---|---|
| **0** | 0 | 1 | 1 |
| **1** | 2 | 12 | 14 |
| **total** | 2 | 13 | |

**Tabla 24:** Matriz de contingencia para la variable DATOS del grupo A.

| Datos | 0 | 1 | total |
|---|---|---|---|
| **0** | 13 | 0 | 13 |
| **1** | 2 | 0 | 2 |
| **total** | 15 | 0 | |

**Tabla 25:** Matriz de contingencia para la variable REPORTADO del grupo A:

| Reportado | 0 | 1 | total |
|---|---|---|---|
| **0** | 13 | 0 | 13 |
| **1** | 0 | 2 | 2 |
| **total** | 13 | 2 | |

Las tablas de la 26, 27, 28 y 29 contienen las matrices de contingencia para cada variable en el Postest respectivamente.

**Tabla 26:** Matriz de contingencia para la variable CLIC del grupo B.

| Clic | 0 | 1 | total |
|---|---|---|---|
| **0** | 7 | 0 | 7 |
| **1** | 5 | 3 | 8 |
| **total** | 12 | 3 | |

**Tabla 27:** Matriz de contingencia para la variable ABIERTO del grupo B.

| Abierto | 0 | 1 | total |
|---|---|---|---|
| **0** | 1 | 1 | 2 |
| **1** | 3 | 10 | 13 |
| **total** | 4 | 11 | |

**Tabla 28:** Matriz de contingencia para la variable DATOS del grupo B.

| Datos | 0 | 1 | total |
|---|---|---|---|
| **0** | 13 | 0 | 13 |
| **1** | 1 | 1 | 2 |
| **total** | 14 | 1 | |

**Tabla 29:** Matriz de contingencia la variable REPORTADO del grupo B.

| Reportado | 0 | 1 | total |
|---|---|---|---|
| **0** | 3 | 11 | 14 |
| **1** | 0 | 1 | 1 |
| **total** | 3 | 12 | |

**Anexo 10:** Configuración GoPhish.

## Descargar e instalar GoPhish desde la página oficial

Pasos:

1. Ir al link oficial de descarga: https://github.com/gophish/gophish/releases
2. Descargar el archivo más reciente o la versión más estable.
3. Descomprimir el archivo en una ruta sin espacios en el nombre.

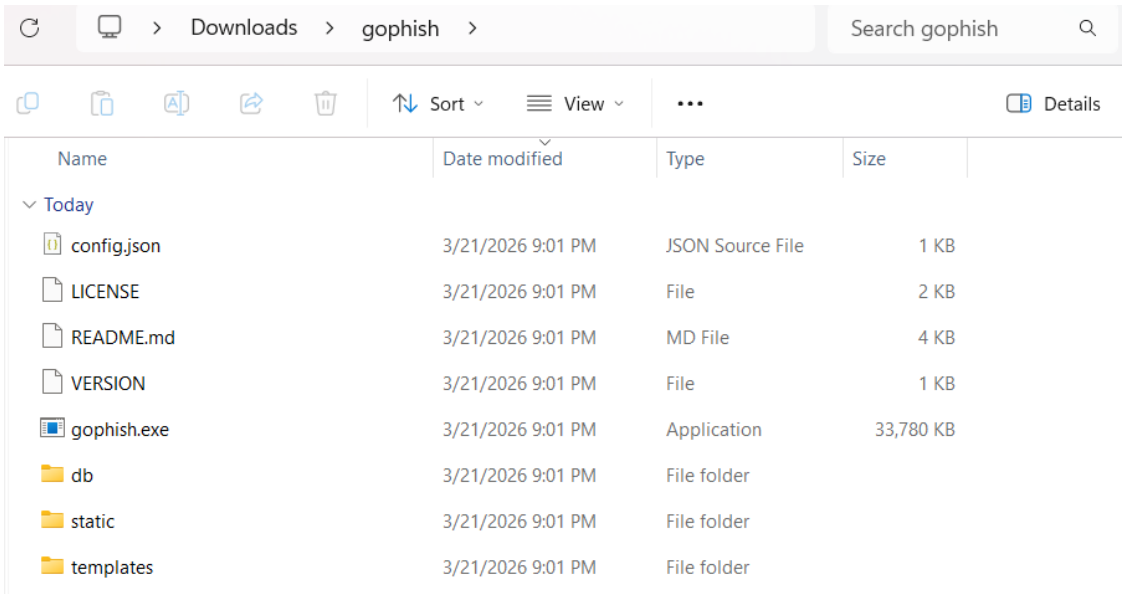



**Figura 11:** Recursos de GoPhish.

## Configuración del config.json

Se debe abrir el config.json con el VS Code y ajustar según las necesidades del entorno. Los campos principales son “admin_server”, “phishing_server” y “db_name”.

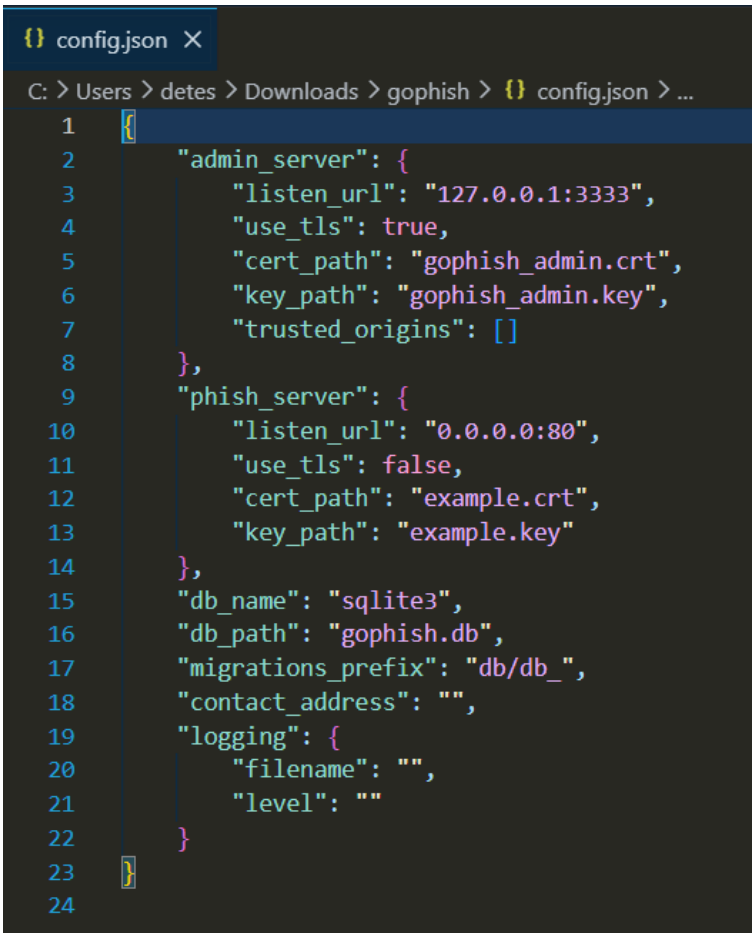



**Figura 12:** Archivo config.json de GoPhish.

Si se está trabajando con Windows, el “listen_url” del admin debe ser 127.0.0.1:3333 para que este solo sea accesible de manera local. En caso de que el puerto 80 esté ocupado por otro servicio se debe cambiar a 0.0.0.0:8080.

## Ejecutar GoPhish como Administrador

Esto es obligatorio en Windows, ya que se necesita de permisos elevados para abrir puertos.

- Clic derecho en gophish.exe y ejecutar como administrador.
- Al ejecutarse por primera vez saldrá lo siguiente:
- Copiar el username y la contraseña que se muestra, ya que solo aparece una vez.

```
OK    20201201000000_0.11.0_account_locked.sql
OK    20220321133237_0.4.1_envelope_sender.sql
time="2026-03-21T23:24:08-05:00" level=info msg="Please login with the username admin and the password a5ea8c482dc9f933"
time="2026-03-21T23:24:08-05:00" level=info msg="Starting IMAP monitor manager"
time="2026-03-21T23:24:08-05:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2026-03-21T23:24:08-05:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2026-03-21T23:24:08-05:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2026-03-21T23:24:08-05:00" level=info msg="Starting new IMAP monitor for user admin"
time="2026-03-21T23:24:08-05:00" level=info msg="TLS Certificate Generation complete"
time="2026-03-21T23:24:08-05:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

**Figura 13:** Logs de la primera ejecución de GoPhish.

## Configurar el firewall de Windows

Ya que GoPhish necesita recibir el tráfico entrante en distintos puertos se debe abrir PowerShell como administrador y ejecutar los siguientes comandos:

- Permitir servidor de phishing en puerto 80.

```
PS C:\Users\detes> New-NetFirewallRule -DisplayName "GoPhish Phish Server" `
>>   -Direction Inbound `
>>   -Protocol TCP `
>>   -LocalPort 80 `
>>   -Action Allow
```

**Figura 14:** Configuración de puertos recomendada.

- En caso de usar un puerto alternativo.

```
PS C:\Users\detes> New-NetFirewallRule -DisplayName "GoPhish Phish Server 8080" `
>>   -Direction Inbound `
>>   -Protocol TCP `
>>   -LocalPort 8080 `
>>   -Action Allow
```

**Figura 15:** Configuración de puertos alternativa.

Al estar corriendo se podrá verificar mediante el navegador que pide aceptar el certificado. Se debe reiniciar la contraseña y se podrá ingresar al dashboard de la herramienta.

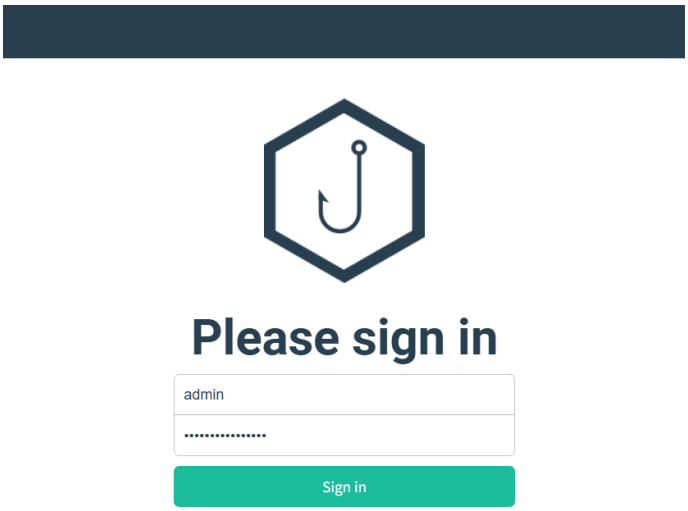



**Figura 16:** Sing In de GoPhish.

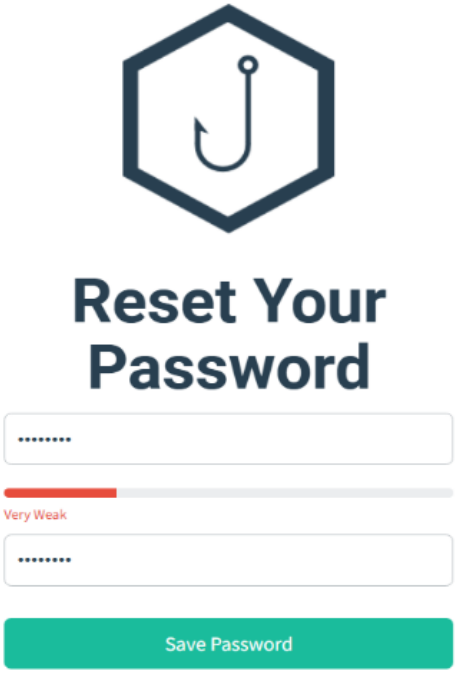



**Figura 17:** Restaurar contraseña de GoPhish.

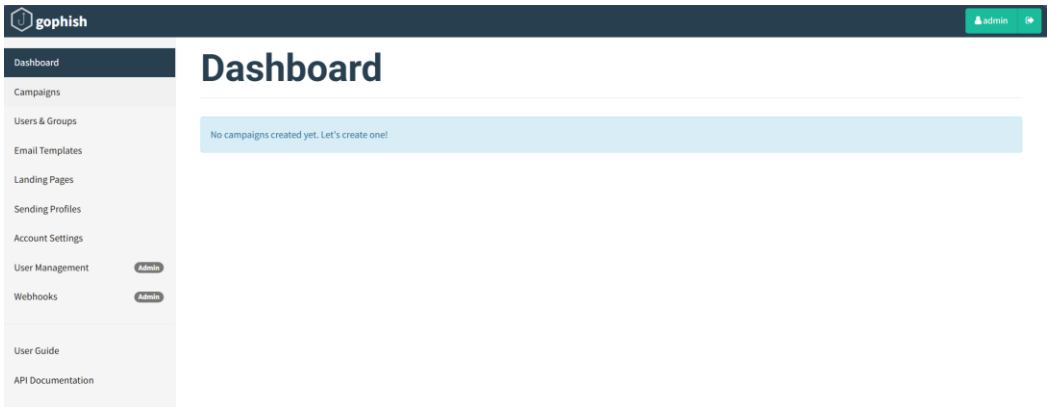



**Figura 18:** Dashboard de GoPhish.

## Creación de Grupos, plantillas y landing page

### Users & Groups

Agregar aquí los usuarios que componen la muestra del Pretest.

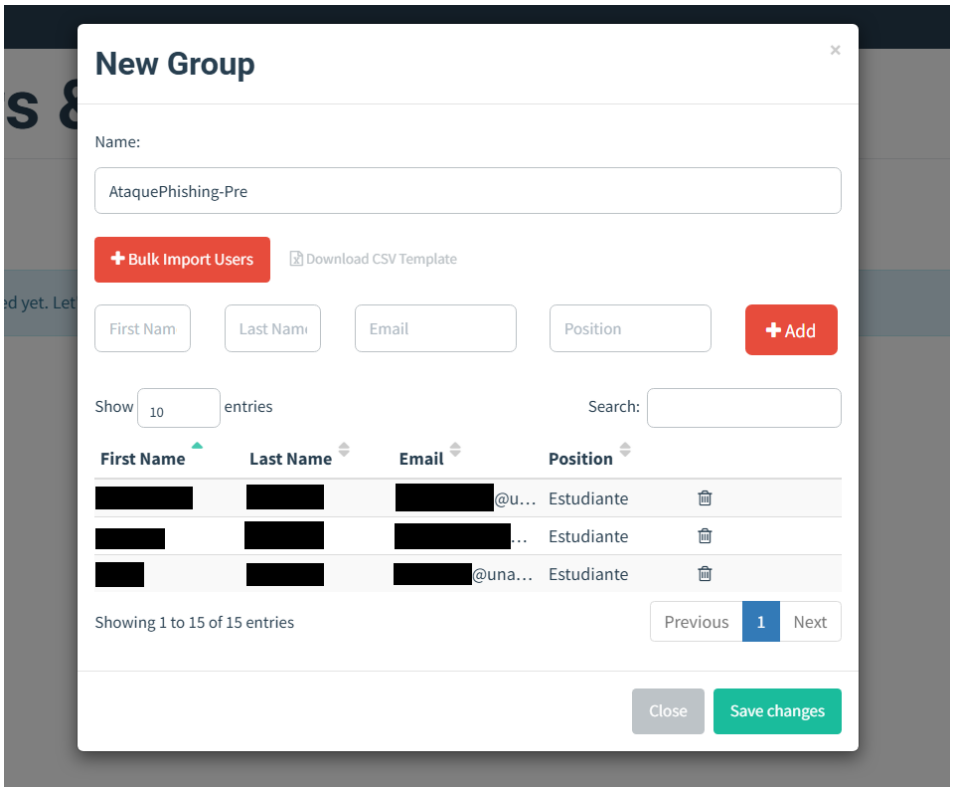



**Figura 19:** Grupo de usuarios del Pretest.

Ahora agregar a un nuevo grupo a los usuarios que componen la muestra del Postest.

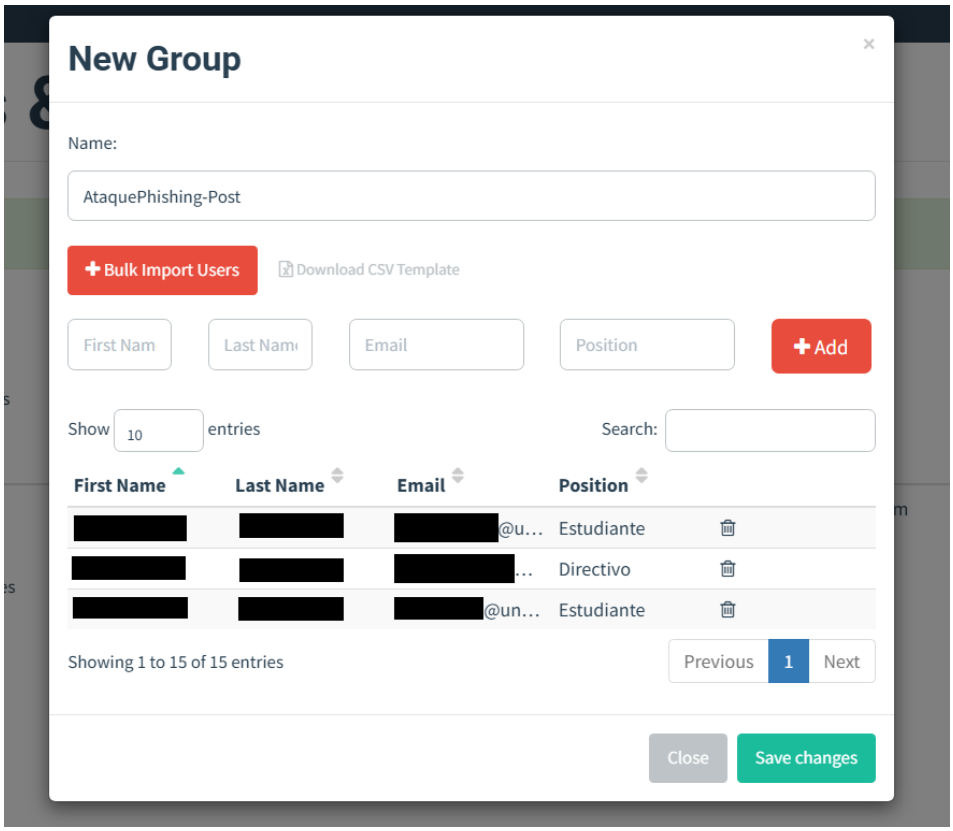



**Figura 20:** Grupo de usuarios del Postest.

## Plantillas de Email

Aquí se va a dar forma al email que se quiere enviar, se recomienda personificar una entidad legítima

# Plantilla Pretest

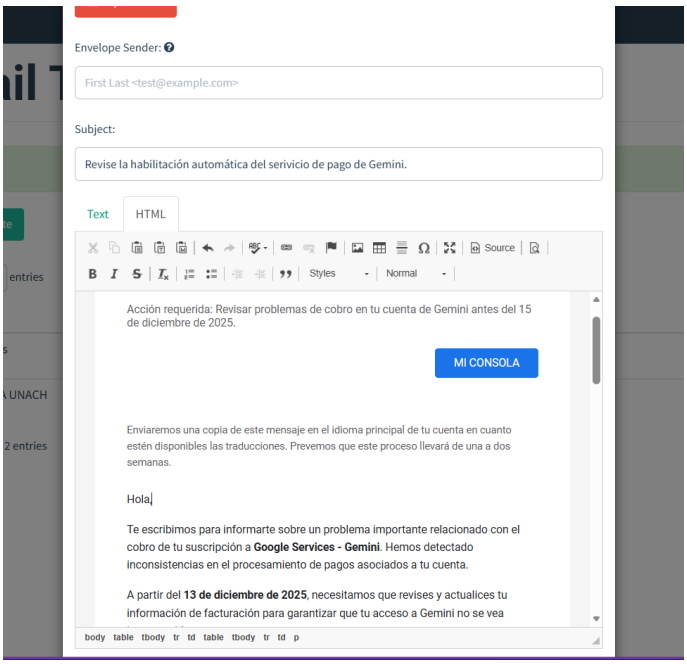



**Figura 21:** Plantilla Pretest.

# Plantilla Postest

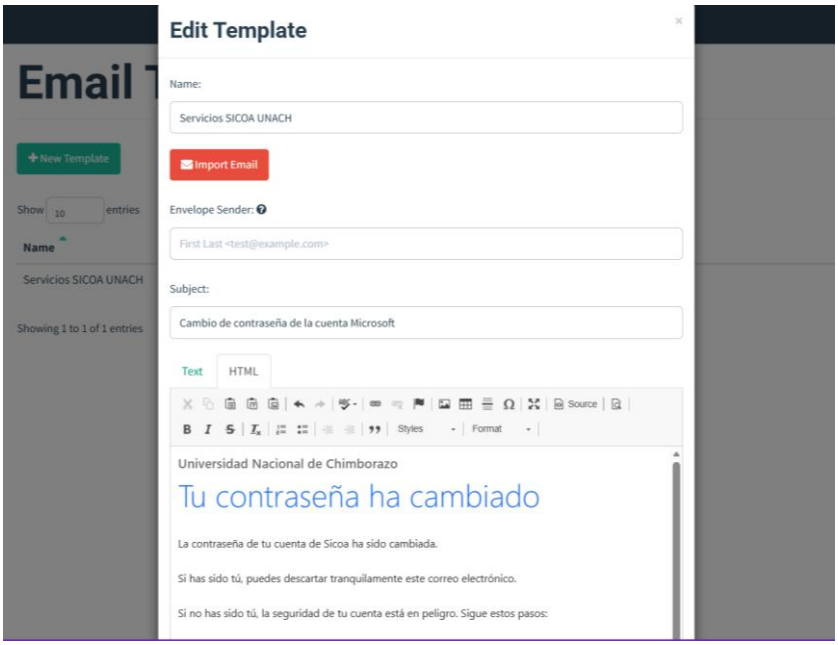



**Figura 22:** Plantilla Postest.

**Anexo 11:** Entrevista al director del DTIC.

**Alain Chacón:** ¿Cuáles son las políticas de seguridad que rigen el correo electrónico?

**Ing. Javier Haro Mgs.:** Políticas de Microsoft (usuario y contraseña) más la doble autenticación, que es una recomendación mandataria de Microsoft.

**Alain Chacón:** ¿Existen protocolos para confirmar la transferencia de datos sensibles?

**Ing. Javier Haro Mgs.:** Existen notificaciones de que se está compartiendo información o archivos, pero sobre el tratamiento o verificación de los datos no disponemos.

**Alain Chacón:** ¿La configuración de Office 365 es la configuración por defecto de Microsoft?

**Ing. Javier Haro Mgs.:** Si, la configuración es la que nos recomienda Microsoft. Microsoft tiene un nivel de cumplimiento donde hace recomendaciones de seguridad, configuración de la plataforma; entonces, nosotros tratamos de adecuarnos a esas recomendaciones.

**Alain Chacón:** ¿Qué criterios utiliza el sistema para clasificar un correo como Spam o Phishing?

**Ing. Javier Haro Mgs.:** Tenemos una atención reactiva, no tenemos aún una lista de sitios para poder restringir; más bien, lo que hacemos es detectar si un correo es malicioso o de phishing y lo ubicamos en listas negras para que los usuarios no lo reciban; adicional a eso, cuando detectamos este tipo de correos, lo que hacemos es trasladar todos los correos que han llegado desde la bandeja de entrada a una bandeja de spam, o en casos más riesgosos los eliminamos.

**Alain Chacón:** ¿Realiza la universidad pruebas periódicas de phishing controlado para evaluar la vulnerabilidad de los usuarios?

Ing. Javier Haro Mgs.: No.

**Alain Chacón:** ¿Existe un programa de formación en ciberseguridad obligatoria para el personal administrativo, docente y estudiantil?

**Ing. Javier Haro Mgs.:** El año anterior (2025) por recomendación del MINTEL, realizamos una capacitación a nivel institucional para que todos los funcionarios tengan una capacitación en ciberseguridad, entonces fue de manera obligatoria organizada por el área de TICS y aprobada por el vicerrectorado administrativo para que todos los funcionarios aprueben esta capacitación.

**Alain Chacón:** ¿Y para los estudiantes?

**Ing. Javier Haro Mgs.:** Para los estudiantes no se ha planificado.

**Alain Chacón:** Si una cuenta de correo es comprometida y comienza a enviar spam ¿Cuál es el tiempo de respuesta promedio y el protocolo de bloqueo automático?

**Ing. Javier Haro Mgs.:** El tiempo de respuesta lo queremos reducir, pero el administrador de Office 365 es notificado por parte de uno de los funcionarios de TI, en este caso el director, para que tome las acciones necesarias para mitigar el tema del correo.

**Alain Chacón:** Esto dentro del personal administrativo, para el personal estudiantil ¿Hay alguna diferencia?

**Ing. Javier Haro Mgs.:** No, ninguna diferencia. Trabajamos sobre el correo indistintamente que sea de estudiantes, docentes o personal administrativo.

**Alain Chacón:** ¿Cuál es el protocolo para dar de baja las cuentas de correo de estudiantes graduados o personal que deja la institución?

**Ing. Javier Haro Mgs.:** Para el personal administrativo y docentes tenemos un documento que debe pasar por las instancias, incluida la de TICS, donde se desactivan las cuentas de acceso a cuentas de servicios institucionales, y también la cuenta del correo electrónico. Adicional, por temas de almacenamiento y espacio, aplicamos una política para que luego de que se hayan graduado, 6 meses después se elimine el correo en el caso de estudiantes.

**Alain Chacón:** Y para los administrativos ¿Cuánto tiempo se quedan inactivas tras la desvinculación?

**Ing. Javier Haro Mgs.:** Las cuentas se quedan inactivas, no las eliminamos por un tema de contraloría que obliga a tener la información 7 años, por lo que solo limitamos el acceso al correo institucional. Se tiene planeado realizar un barrido para que las cuentas que tienen 7 años cumplidos puedan ser eliminadas.

**Alain Chacón:** ¿Existe una vía oficial para reportar ataques de Spam y Phishing?

**Ing. Javier Haro Mgs.:** En el área de TICS tenemos un área llamada mesa de ayuda, que es donde los estudiantes y docentes pueden acercarse y reportar todo tipo de actividad, y hay un correo que se llama mesadeayuda@unach.edu.ec para que podamos atender los requerimientos.

**Alain Chacón:** Sobre dicho correo ¿Se capacita a los estudiantes para que lo utilicen?

**Ing. Javier Haro Mgs.:** No, no ha habido difusión, es algo que solo existe en la universidad.

**Anexo 12:** Entrevista al encargado del sistema de correo electrónico.

**Ing. Aldaz:** En caso de un hackeo, intento de ataque o phishing u otros intentos como spam. Microsoft tiene una herramienta que se llama Microsoft Defender, que bueno es parte de la Universidad Nacional de Chimborazo, de nuestro Tenant contratado como universidad, dentro de esta herramienta existen dos apartados cuarentena y entidades restringidas, Microsoft automáticamente retiene la cuenta que está afectada, la coloca en cuarentena y en entidades restringidas para su posterior revisión.

**Ing. Aldaz:** Entonces como administrador manualmente lo reviso, hay una parte que se llama Explorador dentro de Microsoft Defender, dentro de explorador existen algunos correos que están ya previamente en cuarentena, aquí se los clasifica como correo no deseado, malware, y algunos que no están clasificado, también clasificados por el remitente vinieron y el dominio, se clasifica todo. Como administrador del Tenant de Microsoft, se realiza un seguimiento que es manual, primero lo que se hace es identificar la cuenta y revocar todas las sesiones activas en los dispositivos asociados que están en esa cuenta, se restablece las contraseñas para la cuenta comprometida en este caso eso es como parte de las políticas que se toman, que son políticas no mínimas, pero tampoco son avanzadas como deberían ser.

**Ing. Aldaz:** Ahí también se hace la eliminación de contraseñas en aplicaciones existentes, porque cuando en la cuenta se autentiquen algunos dispositivos o en algunas aplicaciones también es un medio para poder escalar o infectar otras aplicaciones como en este caso Moodle que está conectado con al correo, se hace la eliminación de esas contraseñas ya a nivel más técnico también se le revisa si no tiene el doble factor de autenticación, se le manda a restablecer el doble factor de autenticación para que otra vez la cuenta vuelva a ser segura.

También se le activa o se le configura como medida preventiva, que es lo más importante ya que según mi experiencia he identificado que algunas cuentas que son más vulnerables son aquellas que no tienen el doble factor de autenticación, estas son las que tiene más intentos de hackeo o reciben mucho spam. Por motivos de seguridad el número de teléfono, en caso de no tenerlo se les da un tiempo para poder hacerlo, se les desactiva un tiempo, en este caso algunas políticas que tenemos son de 5 a 7 días máximo.

**Ing. Aldaz:** Si la cuenta se encuentra en entidades restringidas, lo que se realiza es un análisis manual para identificar si es malware, phishing. Como administrador, identifico el correo y realizado una acción que en este caso sería de eliminación masiva de este correo de todas las bandejas de entrada, ya que como es el mismo dominio, se dispersa entre estudiantes, docentes o administrativos. Al hacer esta eliminación de la bandeja de entrada es una forma de mitigar o minimizar la tendencia a hacer clic en el enlace malicioso.

**Alain Chacón:** ¿O sea que se le borra toda la bandeja de entrada al afectado?

**Ing. Aldaz:** No, no se le borra la bandeja de entrada, se borra el correo que llegó a las bandejas de entrada. Como somos los administradores de Microsoft, si les llega a mil personas, de esas mil cuentas se borra el correo malicioso en cada una de ellas.

**Alain Chachón:** ¿De las mil cuentas se elimina ese correo preciso?

**Ing. Aldaz:** El correo como tal, el correo infectado.

**Alain Chacón:** ¿Eso lo hace usted manual?

**Ing. Aldaz:** Si, de forma manual. No tenemos una herramienta, hay otras herramientas más avanzadas que nos ayudarían a hacer automáticamente pero obviamente tienen su costo.

**Ing. Aldaz:** Como parte de esto también se le envía a Microsoft, ya que tiene una opción para enviar y que Microsoft también revise ese correo. Y obviamente yo clasifico ese correo como malicioso, lo envío a Microsoft y ellos mejoran los filtros para ese tipo de correos.

**Alain Chacón:** ¿Algo adicional?

**Ing. Aldaz:** Juntamente con CEDIA, ellos tienen a nivel de universidades, herramientas de análisis de vulnerabilidades que también nos ayudan a identificar este tipo de intentos de ataque. Con ellos se maneja un tema menos técnico, un tema más de reglamento.

**Alain Chacón:** ¿Qué quiere decir eso?

**Ing. Aldaz:** Ellos de alguna manera nos hacen poner énfasis en la Ley de Protección de Datos, ya que a veces estos tipos de correos buscan adquirir datos personales. Hacen mención de que a toda información que se pida mediante correo, también se le envíe unos artículos que mencionan esa ley. Cada correo que se ve comprometido se menciona que se protegió citando sus artículos.

**Ing. Aldaz:** Eso es algo que lo estamos trabajando actualmente. No es todavía una política que ya está como tal en la Universidad. Las políticas establecidas son la revocación y el restablecimiento.

**Ing. Aldaz:** Esas políticas ya son establecidas, no están enunciadas como tal en todo, porque junto con el Departamento de Seguridad todavía están trabajando una consultoría para esclarecer más ese tema. Pero como administrador tomo etas medidas como establece Microsoft. Entonces como tal no están publicada, pero como departamento aquí la hacemos de esa manera.