CENTRO UNIVERSITARIO TECNOLÓGICO CEUTEC

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y SOCIALES

PROYECTO DE GRADUACIÓN

FRAUDE EN EL SISTEMA BANCARIO EN HONDURAS Y SUS MECANISMOS DE PREVENCIÓN

SUSTENTADO POR

AIDA MARIBEL BONILLA CRUZ 30841239

DUSTIN RAMSES AMADOR VARGAS 31951287

MICHELLE MELGAR VÁSQUEZ 31221085

PREVIA INVESTIDURA AL TITULO DE LICENCIATURA EN CONTADURÍA PÚBLICA Y FINANZAS

TEGUCIGALPA HONDURAS, C.A.

ENERO, 2025

CENTRO UNIVERSITARIO TECNOLÓGICO CEUTEC

LICENCIATURA EN CONTADURÍA PÚBLICA Y FINANZAS

AUTORIDADES UNIVERSITARIAS

RECTORA:
ROSALPINA RODRÍGUEZ GUEVARA

VICERRECTOR ACADÉMICO:
JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL:
ROGER MARTÍNEZ MIRALDA

DIRECTORA:
JESSY CAROLINA AYESTAS HERNÁNDEZ

TEGUCIGALPA **HONDURAS, C.A.**

ENERO, 2025

FRAUDE EN EL SISTEMA BANCARIO EN HONDURAS Y SUS MECANISMOS DE PREVENCIÓN

TRABAJO PRESENTADO EN EL CUMPLIMIENTO DE LOS REQUISITOS

EXIGIDOS PARA OPTAR AL TÍTULO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA Y FINANZAS

ASESOR:

YENNY ELIZABETH ANDRADE ÁLVAREZ

TERNA EXAMINADORA:

FAUSTO EFRAÍN FLORES MONCADA
ÁNGELA PAMELA ROMERO PONCE
RAYNEL ENRIQUE LÓPEZ

TEGUCIGALPA **HONDURAS, C.A.**

ENERO, 2025

DERECHOS DE AUTOR

AIDA MARIBEL BONILLA CRUZ

DUSTIN RAMSES AMADOR VARGAS

MICHELLE MELGAR VÁSQUEZ

DEDICATORIA

Este trabajo está dedicado a Dios, quien me brinda la fuerza, la inteligencia y la sabiduría para seguir adelante. A mi familia, por ser mi motor y motivarme a no rendirme. Y, especialmente, a mi hijo Joel David Bonilla, quien es mi mayor inspiración. Espero que él comprenda que cada esfuerzo tiene su recompensa.

.

AIDA MARIBEL BONILLA CRUZ

Le dedico este trabajo primeramente a Dios que me ha dado la fuerza y la oportunidad para seguir adelante hasta este momento, a mi hijo Carlos Adriel, por ser mi inspiración y el motor que me ayuda a salir adelante cada día y a mi familia que me ha apoyado en los momentos más difíciles y siempre ha estado presente motivándome.

MICHELLE MELGAR

Quiero dedicar esta victoria a mis abuelos, quienes durante toda mi vida han sido un pilar fundamental en ella, sin ustedes jamás hubiera logrado ser quien soy; a mi tía, quien con su ejemplo me ha motivado a nunca rendirme y a siempre querer imitarla; a mi madre y hermano, por estar siempre conmigo y a mis amigos que nunca me han dejado caminar solo.
Sin ustedes ninguna victoria tendría valor, ni mi vida tendría sentido.

DUSTIN VARGAS

AGRADECIMIENTOS

Estoy infinitamente agradecida con Dios por sus bendiciones y por ayudarme a realizar uno de mis sueños. El camino fue largo y, sin duda, no fue fácil, pero gracias a Él logré llegar. Quiero dedicar un agradecimiento especial a mi abuela, Paula Ruiz, por su apoyo incondicional y por siempre creer en mí. A mi hijo, Joel David Bonilla, por ser mi mayor motivación, así como a mis hermanos en la fe, amigos y compañeros de trabajo, quienes siempre estuvieron presentes a lo largo de este proceso.

AIDA MARIBEL BONILLA CRUZ

Le agradezco a Dios, quien siempre me ha guiado y me ha bendecido al darme la oportunidad de seguir con mis estudios. A mi familia por apoyarme cuando lo he necesitado a pesar de que no siempre estén de acuerdo con mis decisiones. Y a mi hijo Carlos Adriel, que ilumina mis días y me muestra que cada día es una oportunidad nueva para mejorar y encontrar la felicidad de la vida en las cosas sencillas.

MICHELLE MELGAR

Quiero agradecer a Dios por acampar sobre mi como poderoso gigante e ir delante de mí en cada etapa de mi vida. El honor y la gloria siempre serán solo tuyos.

DUSTIN VARGAS

RESUMEN EJECUTIVO

Este documento es un estudio que tiene como propósito analizar el fraude en el sistema bancario en Honduras y sus mecanismos de prevención, los casos de fraude en el sistema bancario se llevan a cabo a través de la manipulación de los registros bancarios por parte de personal interno o externo a la institución, por lo que se ve afectada la credibilidad, la confianza del cliente, y reputación de la institución.

Esta problemática representa un desafío para el sistema bancario en Honduras, ya que no solo afecta a la institución bancaria también se ven afectados los clientes, la suplantación de identidad, las transacciones no autorizadas por parte del titular de la cuenta, como resultado las instituciones bancarias pierden credibilidad.

Este estudio identifica las medidas necesarias para mitigar el fraude en el sistema bancario mediante la educación financiera a los usuarios, ayudándoles a prevenir posibles fraudes y elevando su nivel de conciencia para su protección. Para ello, se proponen que los medios de difusión de información autorizados por las instituciones bancarias notifiquen que la entidad nunca solicitará claves de acceso y que las únicas páginas autorizadas para realizar transacciones son las oficiales de cada una. Además, se recomienda habilitar la opción para que el usuario pueda bloquear su cuenta desde la página oficial de su banco en caso de detectar movimientos no autorizados.

El fraude bancario es un riesgo significativo que no solo afecta a los usuarios del sistema bancario, está en juego la credibilidad de las instituciones bancarias en Honduras, con la creciente digitalización y el uso masivo del sistema en línea, se han expuesto la vulnerabilidad de los sistemas de seguridad permitiendo que los métodos de fraude tengan un impacto negativo en las finanzas de los usuarios, perdiendo la confianza en el sistema bancario. El aumento de los casos de fraude crea la necesidad de analizar a profundidad el impacto en los usuarios, evaluando la efectividad de las medidas de prevención implementadas por el sistema bancario.

El capítulo presenta un enfoque metodológico mixto que combina técnicas cualitativas y cuantitativas para analizar el impacto del fraude bancario en Honduras, con especial atención a los usuarios de la banca en Tegucigalpa. Se examinan los principales tipos de fraude, como la suplantación de identidad, la clonación de tarjetas y el robo de información, los cuales afectan la confianza en el sistema financiero y provocan pérdidas económicas para instituciones y clientes.

El fraude bancario aumentó tras la pandemia de COVID-19 debido al mayor uso de plataformas digitales, lo que expuso nuevas vulnerabilidades. Los métodos más comunes son el phishing, el skimming y el uso de cuentas "mulas". Para combatirlo, las instituciones financieras implementaron medidas de seguridad como la autenticación multifactorial y la detección de fraudes en tiempo real. Sin embargo, la falta de conocimiento de los usuarios los mantiene expuestos. La CNBS impulsa regulaciones para mitigar el fraude, pero enfrenta retos en la detección temprana y la educación de los usuarios. Los bancos deben reforzar la seguridad y la educación de sus clientes, mientras que el marco legal, aunque sanciona estos delitos, presenta limitaciones en su aplicación. Para combatir el fraude bancario, se proponen cinco estrategias clave:

1. **Fortalecimiento de la ciberseguridad**: Actualización de sistemas de seguridad, autenticación multifactor y detección de fraudes en tiempo real.
2. **Uso de inteligencia artificial (IA)**: Detección de patrones delictivos y previsión de nuevas tácticas mediante aprendizaje continuo.
3. **Educación financiera inclusiva**: Capacitación de usuarios en comunidades rurales y creación de materiales interactivos.
4. **Atención rápida al cliente**: Protocolos para la resolución de casos de fraude y herramientas para bloquear cuentas ante sospechas.
5. **Fortalecimiento regulatorio por la CNBS**: Supervisión rigurosa y sanción a instituciones que incumplan los estándares de seguridad.

   El capítulo propone un plan de contingencia para la banca en línea, enfocado en prevención, atención al cliente y continuidad de servicios. Incluye análisis de riesgos y campañas educativas para proteger datos, prevenir fraudes y fortalecer la seguridad. Su objetivo es reducir la vulnerabilidad de los usuarios y restaurar la confianza en el sistema financiero.

ABSRACT

This document is a study aimed at analyzing fraud in the banking system in Honduras and its prevention mechanisms. Fraud cases in the banking system occur through the manipulation of bank records by internal or external personnel, which affects the credibility, customer trust, and reputation of the institution.

This issue presents a challenge for the banking system in Honduras, as it not only affects the banking institution, but also impacts customers, identity theft, and unauthorized transactions by the account holder. As a result, banking institutions lose credibility.

This study identifies the necessary measures to mitigate fraud in the banking system through financial education for users, helping them prevent potential fraud and raising their awareness for protection. To this end, it is proposed that the media authorized by banking institutions inform the public that the entity will never ask for access credentials and that the only authorized pages for transactions are the official ones. Furthermore, it is recommended to enable an option for users to block their account directly from the bank's official website if they detect unauthorized transactions.

Bank fraud is a significant risk that not only affects the users of the banking system, the credibility of banking institutions in Honduras is at stake, with the growing digitalization and massive use of the online system, but the vulnerability of the security systems also allowing fraud methods to have a negative impact on users' finances, losing trust in the banking system.
The increase in fraud cases creates the need to deeply analyze the impact on users, evaluating the effectiveness of the prevention measures implemented by the banking system.

The Methodology/Process chapter presents a mixed methodological approach, combining qualitative and quantitative techniques to analyze the impact of banking fraud in Honduras.

The chapter presents a mixed methodological approach that combines qualitative and quantitative techniques to analyze the impact of banking fraud in Honduras, with special attention to banking users in Tegucigalpa. The main types of fraud are examined, such as identity theft, card cloning and information theft, which affect trust in the financial system and cause economic losses for institutions and clients.

Bank fraud increased following the COVID-19 pandemic due to the increased use of digital platforms, exposing new vulnerabilities. The most common methods are phishing, skimming and the use of "mule" accounts. To combat this, financial institutions implemented security measures such as multi-factor authentication and real-time fraud detection. However, users' lack of knowledge keeps them exposed. The CNBS pushes regulations to mitigate fraud, but faces challenges in early detection and user education. Banks must reinforce the security and education of their clients, while the legal framework, although it punishes these crimes, has limitations in its application. To combat bank fraud, five key strategies are proposed:

1. Strengthening cybersecurity: Updating security systems, multi-factor authentication and fraud detection in real time.
2. Use of artificial intelligence (AI): Detection of criminal patterns and prediction of new tactics through continuous learning.
3. Inclusive financial education: Training of users in rural communities and creation of interactive materials.
4. Quick customer service: Protocols for resolving fraud cases and tools to block accounts if suspected.
5. Regulatory strengthening by the CNBS: Rigorous supervision and sanctioning of institutions that fail to comply with security standards.

The chapter proposes a contingency plan for online banking, focused on prevention, customer service and continuity of services. It includes risk analysis and educational campaigns to protect data, prevent fraud and strengthen security. Its objective is to reduce the vulnerability of users and restore confidence in the financial system.

Tabla de Contenido

GLOSARIO

- **Ciberseguridad:** Conjunto de prácticas y tecnologías implementadas por las instituciones bancarias para protegerse de ataques cibernéticos y fraudes en línea.
- **Cuentas mulas**: Son cuentas bancarias abiertas a nombre de terceros que actúan como intermediarios para recibir dinero de origen fraudulento o para transferirlo a otros destinos.
- **El fraude electrónico**: Es un tipo de estafa en la que se utilizan comunicaciones electrónicas para engañar a alguien a fin de que envíe dinero o información confidencial.
- **Fraude bancario:** Es una conducta delictiva que implica la manipulación o fraude en el sistema financiero para lograr ganancias económicas de las entidades bancarias o los usuarios en Honduras.
- **Fraude interno**: Fraude cometido por empleados de las instituciones financieras, como la manipulación de registros o la sustracción de fondos de cuentas bancarias de clientes.
- **La Comisión Nacional de Bancos y Seguros (CNBS)**: Entidad reguladora del sistema financiero en Honduras, responsable de supervisar y controlar las instituciones bancarias, así como de implementar medidas contra el fraude.
- **Medidas preventivas:** Acciones implementadas por las instituciones financieras, como campañas de educación financiera y tecnologías de seguridad, para prevenir fraudes bancarios.
- **Monitoreo de transacciones**: Proceso mediante el cual las instituciones bancarias vigilan las operaciones realizadas por sus clientes para detectar actividades sospechosas o fraudulentas.
- **Phishing:** Es un tipo común de ciberataque que se dirige a las personas a través del correo electrónico, mensajes de texto, llamadas telefónicas y otras formas de comunicación, conlleva el uso de la manipulación psicológica y el engaño mediante, los cuales los agentes se hacen pasar por entidades de buena reputación para embaucar a los usuarios y lograr que realicen acciones específicas.
- **Robo de datos bancarios**: Es la acción de sustraer información de los clientes como números de cuenta, claves de acceso, y códigos de seguridad para realizar los fraudes.

- **Skimming:** Es un tipo de fraude que consiste en robar información de tarjetas de crédito o débito para realizar compras o retirar dinero.
- **Suplantación de identidad**: Acción de hacerse pasar por otra persona para acceder a sus cuentas bancarias y realizar actividades fraudulentas.
- **Transacciones no autorizadas**: Movimientos de dinero en cuentas bancarias realizados sin el consentimiento del titular de la cuenta, frecuentemente resultado de fraude.

CAPÍTULO l. INTRODUCCIÓN

El fraude en el sistema bancario en Honduras ha ganado importancia en los últimos años, impactando a las entidades financieras y a los usuarios. Este tipo de fraude se manifiesta en distintas modalidades: la falsificación de identidad, el acceso no autorizado a las cuentas bancarias, la clonación de las tarjetas de créditos y esto debido a la vulnerabilidad del sistema, etc.

El avance tecnológico y la falta de medidas de seguridad han generado vulnerabilidades en los sistemas financieros, dando lugar a nuevas tácticas de fraude provocando la desconfianza de los usuarios. A pesar del progreso del sistema bancario hondureño, es necesario implementar estrategias eficaces para prevenir y detectar fraudes. Asimismo, es fundamental examinar las causas, las repercusiones y las posibles soluciones para mitigar este problema.

Por su parte la Comisión Nacional de Banco y Seguros (CNBS) mediante la resolución GRD No.247/23-03-2023 amplió los lineamientos mínimos con los que deben contar las instituciones supervisadas para prevenir y mitigar la ocurrencia de fraudes y estafas cibernéticas en contra del usuario financiero, cuyo objetivo es establecer controles para mitigar la ocurrencia de fraudes, así mismo crear conciencia para la prevención de estos eventos. En el presente documento se detallan estos lineamientos.

En el Capítulo I se aborda como el fraude en el sistema bancario no solo impacta económicamente a los usuarios y a las instituciones, sino que también tiene repercusiones en la reputación y estabilidad de todo el sector. Este estudio se centra en identificar las causas y consecuencias del fraude bancario, así como en explorar las estrategias más efectivas para su prevención y detección. Además, se analiza la importancia de la educación financiera y la implementación de tecnologías de seguridad avanzadas para mitigar estos riesgos, con el objetivo de proponer recomendaciones que fortalezcan la confianza de los usuarios en el sistema bancario hondureño.

En el Capítulo II detalla como el fraude bancario representa una creciente amenaza para la seguridad y estabilidad del sistema financiero, especialmente en un contexto de rápida adopción de servicios digitales y bancarios en línea. La falta de medidas de seguridad adecuadas y la insuficiente educación financiera entre los usuarios han generado un ambiente vulnerable, facilitando la aparición de diversas tácticas de fraude, como el robo de identidad, el phishing y el acceso no autorizado a cuentas.

En el Capítulo III se plantea el objetivo general y los objetivos específicos de la investigación. Se analiza el impacto del fraude bancario en los usuarios de la banca en línea en Honduras, evaluando la efectividad de los mecanismos de prevención implementados por las instituciones bancarias. Además, se identifican los métodos de fraude más comunes, se mide su impacto en el bienestar de los usuarios y se examinan las estrategias preventivas actuales. El propósito es proponer mejoras que fortalezcan la seguridad financiera, las políticas de protección de datos y la confianza en el sistema bancario nacional.

En el Capítulo IV se detalla como el fraude bancario ha evolucionado a lo largo del tiempo, adoptando nuevas técnicas con los avances tecnológicos. Definiéndolo como un delito que implica manipulación para obtener beneficios económicos de forma ilícita. Además, se presentan los métodos más comunes, como el phishing, el robo de identidad y el fraude interno, así como estadísticas y casos relevantes a nivel global y en Honduras. También se analiza el rol de las instituciones bancarias y el marco legal en la prevención de estos delitos, destacando la necesidad de fortalecer la seguridad financiera y educar a los usuarios.

El sistema bancario se ha caracterizado por la estabilidad, no obstante, en los últimos años han enfrentado crisis derivadas de significativos fraudes bancarios que han marcado su historia. Entre los más relevantes se encuentran la "fiebre crediticia" de los años 90, que resultó en la quiebra de varios bancos debido a la falta de supervisión y manejo irregular de los fondos; la liquidación forzosa del Banco Continental en 2015 por operaciones no autorizadas; un aumento en las estafas bancarias en línea registrado en 2023.

En el Capítulo V se especifica la metodología adoptada, que combina enfoques cualitativos y cuantitativos para realizar un análisis integral del fraude bancario en Honduras. Se emplean herramientas como la revisión de literatura, análisis de datos secundarios y encuestas a usuarios

de banca en línea. El enfoque mixto permite analizar tanto los datos estadísticos relacionados con la incidencia y pérdidas económicas del fraude, como las percepciones de los usuarios y las prácticas de seguridad de las instituciones financieras. Además, se identifican los métodos de fraude más comunes y las vulnerabilidades del sistema bancario, con el fin de comprender el impacto de este fenómeno y proponer estrategias para mitigarlo.

La población y muestra como el fraude bancario ha impactado a los usuarios, a las instituciones financieras y a los empleados de las instituciones bancarias, se incluye a los principales bancos del país, además se han considerado a los usuarios que han enfrentado pérdidas, robo de identidad, así como los empleados que se desempeñan en departamento claves donde pueden prevenir la detención del fraude, se destaca la labor del ente regulador la Comisión Nacional de Bancos y Seguros (CNBS), que implementa directrices para proteger a los usuarios y mantener la estabilidad del sistema financiero.

En el Capítulo VI**:** se presenta los resultados y el análisis de las encuestas realizadas a usuarios del sistema bancario en Tegucigalpa.

En el Capítulo VII y VIII: se desarrollan las conclusiones y recomendaciones derivadas del análisis detallado de la información recopilada a través de encuestas.

En el Capítulo IX: contiene las referencias bibliográficas utilizadas en la investigación.

En el Capítulo X: incluye los anexos correspondientes a la investigación.

En el Capítulo XI: se expone la aplicabilidad de los hallazgos en el sistema bancario hondureño.

CAPÍTULO ll. PLANTEAMIENTO DEL PROBLEMA

2.1 ANTECEDENTES

A lo largo de los años, el fraude en el sistema bancario hondureño ha experimentado múltiples manifestaciones, afectadas por elementos económicos, políticos y sociales. Desde que se fundó el Banco Atlántida en 1913, más de 30 bancos privados en Honduras, decenas de cooperativas y otras instituciones financieras se han declarado en quiebra, gran parte de las liquidaciones están asociadas a la corrupción, fraude e ineficiencias administrativas. (CNBS, (repositorio.cepal.org), 2006)

A fines de los años 1990, Honduras enfrentó una crisis bancaria que resultó en el colapso de varios bancos, causada por la falta de regulación y supervisión, así como por las malas prácticas que propiciaron el fraude y el robo. Durante los años 1998-2003, el sistema financiero hondureño sufrió pérdidas millonarias debido a la quiebra de instituciones bancarias y asociaciones financieras. Los casos más sonados involucraron a Banca Corporativa (BANCORP), Banco de Crédito y Seguros (BANCRESER) y Banco Capital.
El Gobierno de Honduras se vio obligado a establecer fideicomisos de miles de millones de lempiras con el fin de prevenir un desorden en la economía nacional y devolver sus ahorros a los deudores. . (https://www.elpulso.hn/2017/05/16/crisis-bancaria-estafa-corrupcion-e-impunidad-14/, 2017)

El 31 de marzo del año 2023 el Ministerio Público presentó un reporte el cual detallaba que, en el transcurso de 3 meses, se habían recibido más de 100 denuncias por delitos financieros e informáticos, reportando que sus víctimas habían sido estafadas a través de medios electrónicos los cuales tenían como finalidad extraer el dinero de sus cuentas bancarias.

Las pérdidas alcanzadas en dichos fraudes rondaban entre L.10,000.00 a L.1,000,000.00; esto sucedía a raíz de que los usuarios financieros proporcionaban información personal a través de cuentas de banco falsas, correos electrónicos, llamadas o mensajes por diferentes medios de contacto. Cabe destacar que, según el Código Penal de Honduras, en su artículo 398 detalla que “El delito de acceso no autorizado a sistemas informáticos se paga con cárcel o multa”.

2.2 FORMULACIÓN DEL PROBLEMA

El fraude bancario es un problema de alcance global que afecta la economía de los países y pone en riesgo la seguridad financiera de sus ciudadanos, causando pérdidas significativas en el patrimonio tanto de los usuarios como de las instituciones. En Honduras, el sector bancario ha mostrado un crecimiento notable, acompañado de una progresiva digitalización de sus servicios. Sin embargo, este avance ha traído consigo un incremento en los casos de fraude, lo cual plantea serias amenazas para la estabilidad financiera de los clientes y la integridad del sistema bancario.

El fraude en el sistema bancario se puede apreciar de diversas maneras, tales como: la simulación de identidad, las operaciones no autorizadas y la aplicación de tecnología para la obtención de información.

La Comisión Nacional de Banca y Seguros como ente regulador ha implementado estrategias para minimizar los riesgos de fraude cibernético a través de los canales digitales que ofrecen a sus usuarios financieros. Esta estrategia debe estar fundamentada en una evaluación de riesgos conjunta con las unidades de negocio y las funciones de vigilancia correspondientes, alineadas con las políticas de seguridad de cada institución.

Las instituciones supervisadas deben disponer de sistemas para detectar nuevas formas de fraudes y estafas cibernéticas que estén ocurriendo en el país y en la zona, con el propósito de incrementar el análisis de riesgos en canales digitales e incluir en las campañas de sensibilización, alertas que puedan salvaguardar al usuario financiero de ser objeto de engaños.

Entre las prácticas fraudulentas más comunes se pueden mencionar:

- Robo de identidad y apropiación de cuentas
- Estafas de phishing e ingeniería social
- Fraude con tarjeta
- Fraude bancario online

2.3 PREGUNTAS DE INVESTIGACIÓN

Las preguntas de investigación requeridas para elaborar este estudio se detallan a continuación y serán orientadas para responder a la interrogante:

¿Cómo ha impactado el fraude en el sistema bancario en Honduras y cuáles sus mecanismos de prevención?

1. ¿Cuáles son las formas de fraude bancario más comunes en Honduras?
2. ¿Qué medios se utilizan para realizar el fraude bancario?
3. ¿Cómo afectan los fraudes la confianza de los usuarios en las instituciones bancarias en Honduras?
4. ¿Qué grado de conocimiento tienen los usuarios a los mecanismos de prevención de fraude bancario en su institución financiera y que medidas deben tomarse para mejorar su concientización sobre estos mecanismos?

2.4 HIPÓTESIS Y VARIABLES DE INVESTIGACIÓN

2.4.1 HIPÓTESIS

Se establece la siguiente hipótesis de investigación:

"La falta de actualización en sistemas de seguridad digital en las instituciones bancarias es un factor que incrementa la frecuencia de fraudes."

Esta hipótesis se fundamenta en los informes de la CNBS, los cuales revelan que en los últimos años ha habido un aumento en los casos de fraude en instituciones bancarias, tanto en aquellas que no han actualizado sus sistemas como en las que ya cuentan con tecnología de vanguardia. Además, se consideran las medidas de seguridad implementadas por la banca dirigidas a proteger al usuario.

En esta investigación se podrá confirmar o refutar la hipótesis, mediante el análisis de encuestas realizadas a los usuarios y la información proporcionada por el ente regulador, la Comisión Nacional de Banca y Seguros. Asimismo, se deben considerar que el fraude va más allá de los

devastadores golpes financieros.

El perjuicio a la imagen y la degradación de la confianza y la satisfacción del cliente pueden generar un efecto negativo, incluso puede haber demandas por los daños ocasionados a los usuarios.

2.4.2 VARIABLES DE INVESTIGACIÓN

Para abordar el estudio del fraude bancario en Honduras, es esencial identificar y analizar diversos factores que influyen en su ocurrencia y evolución. Entre los factores clave se encuentran las vulnerabilidades tecnológicas de los sistemas bancarios, como la falta de actualización de software y la seguridad de las plataformas en línea, etc.

2.4.2.1 VARIABLES DEPENDIENTES

Las variables dependientes son aquellas que están sujetas a cambios o variaciones en función de las variables independientes o los factores que se manipulan o controlan en un estudio. Estas se utilizan para evaluar el impacto o la relación entre los factores de interés y los resultados medibles.
En el marco de las repercusiones del fraude en el sistema bancario esta variable podría formularse de la siguiente manera:

1. **Pérdidas financieras de las víctimas del fraude bancario**: Esta variable mide el monto de dinero que los usuarios pierden debido a incidentes de fraude bancario. Se ve directamente influenciada por la frecuencia y la magnitud de los fraudes que ocurren en las instituciones bancarias.
2. **El número de reportes de fraude bancario**: Esta variable refleja el volumen de casos de fraude que son detectados y reportados por las instituciones bancarias. Está influenciada por la capacidad de los bancos para identificar fraudes (medidas de seguridad), la educación de los usuarios y las tácticas de fraude utilizadas.

2.4.2.2 VARIABLES INDEPENDIENTES

Las variables de estudio independientes son aquellas que se alteran o se ven como causantes de un efecto en el marco de una investigación.

1. La naturaleza del tipo de fraude bancario: Esta variable afecta el tiempo de investigación y la resolución del caso, ya que el fraude interno, por involucrar a empleados con acceso a los sistemas y procesos, puede ser más difícil de detectar y resolver, alargando el tiempo de investigación. En cambio, el fraude externo, cometido por personas fuera de la institución, suele ser más directo de investigar, lo que generalmente acelera su resolución.
2. Áreas del sistema bancario que interactúan con los usuarios o procesan la información: Estas áreas son susceptibles a cometer errores o fraudes debido a la interacción directa con los usuarios o la manipulación de datos.

2.4.3 DELIMITACIÓN

Esta investigación se llevará a cabo en la ciudad de Tegucigalpa, M.D.C., durante el periodo comprendido entre octubre y diciembre de 2024. El enfoque principal de este estudio será el fraude en el sistema bancario de Honduras, analizando tanto las causas que favorecen su ocurrencia como los mecanismos de prevención implementados por las instituciones financieras. Se estudiarán diversas modalidades de fraude que afectan a los usuarios y a las entidades bancarias, tales como el fraude con tarjetas de crédito, el phishing, el robo de identidad y las estafas en línea. Además, se explorará el impacto del fraude en la economía nacional, con especial atención a las pérdidas financieras sufridas por los clientes y las repercusiones para la estabilidad del sistema bancario.

La investigación también incluirá un análisis de las políticas y medidas de seguridad adoptadas por las instituciones bancarias hondureñas, así como la eficacia de las tecnologías implementadas para detectar y prevenir fraudes. Asimismo, se considerará la educación financiera de los usuarios como un factor clave para mitigar el fraude, evaluando cómo los bancos informan y capacitan a

sus clientes para identificar y prevenir fraudes. A través de encuestas a usuarios de diferentes entidades bancarias y el análisis de información proporcionada por la Comisión Nacional de Banca y Seguros (CNBS), se obtendrán datos relevantes para comprender el panorama actual del fraude bancario en el país y la efectividad de las estrategias de prevención en vigor.

2.4.4 JUSTIFICACIÓN

El fraude bancario es uno de los principales riesgos que enfrentan tanto las instituciones financieras como sus usuarios. En Honduras, este fenómeno ha tomado relevancia en los últimos años, debido en gran parte a la expansión de plataformas digitales y al acceso masivo a servicios bancarios en línea. Sin embargo, esta creciente digitalización también ha expuesto nuevas vulnerabilidades en los sistemas de seguridad, facilitando la aplicación de métodos sofisticados para cometer actos ilícitos. Estas prácticas afectan no solo las finanzas de los usuarios, sino también su bienestar emocional y su confianza en el sistema bancario, un factor clave para la estabilidad y el desarrollo económico del país.

Las estadísticas recientes indican un incremento en los casos de fraude bancario en Honduras, lo cual genera pérdidas significativas para las instituciones y los usuarios afectados. Estas pérdidas, combinadas con la falta de conocimiento sobre prácticas seguras por parte de los usuarios, subrayan la necesidad de estudiar a fondo el impacto del fraude bancario en el bienestar financiero y emocional de los clientes, así como de analizar los mecanismos actuales de prevención implementados por las instituciones financieras.

CAPÍTULO lll. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar el impacto de fraudes bancarios en los usuarios de banca en línea de Honduras, así como evaluar la efectividad de los mecanismos de prevención implementados por las instituciones bancarias, con el fin de proponer estrategias más efectivas que fortalezcan la seguridad financiera de los clientes, mejoren las políticas de protección de datos y refuercen la confianza del público en el sistema bancario nacional.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los métodos y medios utilizados con mayor frecuencia para cometer fraudes bancarios en Honduras, con el fin de proponer alternativas de prevención.
- Evaluar el impacto de los fraudes bancarios en el bienestar de los usuarios financieros en Honduras con el fin de conocer la cantidad de víctimas de fraude bancario
- Identificar los mecanismos de prevención implementados por las instituciones bancarias ante casos de fraudes bancarios para conocer el impacto que estos tienen en la educación financiera del usuario.

CAPÍTULO IV. MARCO TEÓRICO

El fraude bancario ha existido a lo largo de la historia, pero sus métodos y técnicas han evolucionado al ritmo de los avances tecnológicos de la era digital. Esto obliga a los usuarios bancarios a estar cada vez más alertas. En Honduras, el sector bancario enfrenta el desafío de implementar herramientas más efectivas y educar continuamente a los usuarios sobre cómo prevenir estos fraudes y evitar caer en sus tácticas.

El marco teórico de la presente investigación está estructurado así:

- Historia del Fraude Bancario
- ¿Qué es el fraude bancario?
- Métodos y técnicas más comunes
- Principales fraudes bancarios ocurridos a nivel mundial
- Principales casos de fraudes bancarios en Honduras
- Estadísticas globales sobre los fraudes bancarios.
- Estadísticas sobre fraudes bancarios en Honduras
- El rol y la responsabilidad de las Instituciones bancarias
- Marco Legal de Honduras

4.1 HISTORIA DEL FRAUDE BANCARIO

No existen registros históricos que documenten el primer caso de fraude en la historia mundial; sin embargo, es de entendimiento común que, tan pronto como un ser humano adquirió la posesión de un bien otro probablemente lo codició y trató de obtenerlo mediante engaños.

Sin embargo, diversos documentos legislativos antiguos ya hacen referencia a este tipo de acciones. Por ejemplo, el Código de Hammurabi sancionaba la venta de objetos robados y la alteración de pesas y medidas en el comercio. De manera similar, en las Leyes de Manú se equiparaba el robo con la venta de un bien ajeno, y se castigaba al que vendiera productos de mala calidad, como grano adulterado por uno bueno, hilo de algodón como si fuera de seda, o hierro como si fuera plata.

En cambio, para los romanos, el fraude se entendía como el dolo malo, definido como toda astucia, falacia o maquinación empleada para engañar, burlar o alucinar a otros. Además, incluía tanto la apropiación indebida como la sustracción de bienes, así como las violaciones de posiciones obtenidas mediante engaño y astucia, entre las que se destacaba el acto de obtener dinero simulando ser un acreedor.

No fue sino hasta principios del siglo XIX que se logró definir claramente la separación del fraude como un delito contra el patrimonio, vinculando las falsedades con la protección de la fe pública. En este proceso de conceptualización del fraude, tiene especial relevancia la Ley francesa de julio de 1791, que sirvió de inspiración para el artículo 405 del Código Penal francés napoleónico de 1810. Según este artículo, comete el delito de escroquerie "cualquier persona que, valiéndose de nombres o calidades falsas, o empleando maniobras fraudulentas, logre persuadir a otros sobre la existencia de empresas ficticias, un poder o crédito ilusorio, entre otros". (pierce, 2024)

Fue en la segunda mitad del siglo XIX cuando se logró un concepto genérico de fraude. El Código Penal alemán de 1871, en su párrafo 263, establece que comete el delito de fraude quien, con la intención de obtener para sí o para un tercero un beneficio patrimonial ilícito, causa un perjuicio en el patrimonio de otro, provocando o no evitando un error, ya sea mediante la desfiguración u ocultación de hechos verdaderos. Estos mismos términos fueron adoptados posteriormente por los Códigos Penales de Italia y Suiza. (pierce, 2024)

4.2 ¿QUÉ ES EL FRAUDE BANCARIO?

Antes de definir como tal el termino de fraude bancario, es necesario conocer su definición general, ya que de este se originan diferentes tipos, cambiando su operación, pero no su propósito, el cual se conoce de forma popular como el poder de conseguir su propio bien económico por medio de la manipulación de cualquier tipo hacia otra persona, extrayéndole los recursos por los cuales ha trabajado. Dicho esto, proseguimos a las definiciones:

La Comisión Nacional de Bancos y Seguros define al fraude como “Cualquier acción cometida intencionadamente para obtener ganancias ilícitas o de forma, con intereses de alguna entidad o de un tercero”. (CNBS, 2024)

Sin embargo, el código penal menciona la definición y las sanciones de estafa, cabe resaltar que el fraude y la estafa en términos legales no comprenden las mismas acciones. Se le conoce como fraude a una serie de actividades delictivas, en donde, todas involucran el engaño que se le realiza con la intención de obtener un beneficio injusto o ilegal. El fraude puede ocurrir en diversas situaciones, desde el ámbito de seguros hasta el campo financiero. Por otro lado, la estafa es una subcategoría del fraude, la cual, implica engañar a alguien para que entregue su dinero o bienes de manera voluntaria, aunque su base en información sea falsa o engañosa. La estafa generalmente implica un grado de manipulación interpersonal y explotación de la confianza. (Aclerk, 2024)

El código penal de Honduras solo sanciona la estafa, como se puede ver en el capítulo VI “Estafas y otros fraudes” en el artículo 365 lo define como: “Comete el delito de estafa quien, con nombre supuesto, falsos títulos, influencia o calidad simulada, abuso de confianza, fingiéndose dueño de bienes, créditos, empresas o negociaciones o valiéndose de cualquier artificio, astucia o engaño, indujere a otro en error defraudándolo en provecho propio o ajeno”. (Honduras, 2024)

Se subraya que se comete delito de estafa en los siguientes casos:

1. Quien con el propósito de obtener un provecho ilícito le consigue la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante una manipulación informática o el uso de otro artificio semejante.
2. Quien, utilizando ilegítimamente tarjeta de crédito o débito, cheque, pagare, letra de cambio, los datos obrantes en cualquiera de ellos o cualquier otra forma de pago similar, realiza con ánimo de lucro operaciones en perjuicio de su titular o de un tercero. (Penal, 2024)

4.3 MÉTODOS Y TÉCNICAS MÁS COMUNES DEL FRAUDE BANCARIO.

Existen distintos métodos que los delincuentes actuales utilizan para realizar fraudes y estafas a usuarios bancarios, varias prácticas se vienen realizando desde el siglo anterior. Sin embargo, los métodos y mecanismos han aumentado y se han mejorado durante la era digital, en especial durante la Pandemia del COVID 19, en donde debido al confinamiento que se experimentó a nivel mundial, todas las actividades diarias pasaron de ser presenciales a ser en línea. A continuación, se dará a conocer las practicas más comunes: (CNBS, 2024) (Microblink, 2024)

1. **Robo de identidad y apropiación de cuentas:** Ambas acciones tienen un objetivo común que es apropiarse de los activos financieros de otra persona.
    - El robo de identidad: Es cuando un estafador roba la información de identificación personal de un individuo para abrir una nueva cuenta bancaria o realizar otras actividades fraudulentas
    - La apropiación de cuentas: Se produce cuando se obtiene acceso no autorizado a las cuentas online de un usuario bancario para cometer transacciones fraudulentas.
2. **Fraude con tarjeta:** Es uno de los métodos más utilizados de usurpación de identidad. Se puede producir como perdida o el robo de tarjetas:
    - Skimming: Es la captura de datos de tarjetas de crédito por medio de la banda magnética mediante el uso de tecnologías especiales.
    - Clonación: Es cuando se obtienen los datos de una tarjeta de crédito valida en donde se superponen a una tarjeta en blanco o se utiliza por otro método.
3. **Fraude en préstamo y crédito:** Es cuando se usurpa la identidad con el propósito de obtener un préstamo o una línea de crédito.
4. **Fraude interno:** Se estima que el 50% de los fraudes bancarios proviene del fraude interno por los empleados de la institución bancaria. Las prácticas que más se observan es la malversación de activos, lavado de dinero, robo de datos y fraude por apropiación indebida de bienes.
5. **Fraude bancario online o digital**: En el cual incluye el uso de programas maliciosos para realizar apropiaciones de cuentas, por ejemplo, por medio de transferencias bancarias o fraude de anticipos.

6. **Fraude o estafas por ingeniería social**: En estos casos los estafadores se hacen pasar por algún familiar o entidad válida para solicitar información personal y lleva a cabo la manipulación. Tales prácticas son:
    - Vishing: Es un tipo de fraude que se realiza por medio de llamadas, las cuales son falsas o contienen audios engañosos.
    - Smishing: Es un tipo de fraude por medio de mensajes de texto falsos que llegan a tu teléfono, contienen páginas webs fraudulentas que desean obtener tu información bancaria o promociones para que hagas compras realizando transferencias bancarias.
    - Phishing: Es un tipo de fraude por medio de correos electrónicos falsos donde te remiten un link para ingresar a páginas webs fraudulentas y robar tu información personal.
7. **Pharming:** Este consta de la réplica de las plataformas y páginas web para que los usuarios se confundan con dichas interfaces con las entidades bancarias y puedan facilitar su información personal. Se debe sospechar de una página web si al ingresar, su dirección web se transforma automáticamente en una IP numérica y cuando en la barra de direcciones no se observa los certificados de seguridad de los sitios webs.
8. **Key logger:** También se le puede conocer como capturador de teclado este se trata de programas o dispositivos físicos que se instalan en la computadora u aparato electrónico para capturar lo que escribe un usuario, para que dicha información sea utilizada posteriormente. Este tipo de hardware se conectan en las computadoras o aparatos electrónicos por medio de un puerto USB y almacena los datos que sean ingresados al computador mediante el teclado.
9. **Cuentas mulas:** Son cuentas bancarias abiertas a nombre de terceros que actúan como intermediarios para recibir dinero de origen fraudulento o para transferirlo a otros destinos. Se les denomina 'cuentas mulas' porque funcionan como un vehículo para el transporte de fondos ilícitos de un punto a otro. En ocasiones, los delincuentes abren estas cuentas utilizando datos robados de otras personas. El titular de la cuenta mula recibirá en su cuenta dinero de origen ilegal, el cual luego será transferido a otras cuentas, ocultando así el rastro de los fondos. (Garrote, 2024)

4.4 PRINCIPALES FRAUDES BANCARIOS OCURRIDOS A NIVEL MUNDIAL

A nivel mundial, el fraude bancario ha evolucionado a lo largo de los años, adoptando nuevas tácticas. Sin embargo, las víctimas suelen ser aquellas personas que no toman las debidas precauciones para proteger sus datos personales y financieros. En caso de entidades financieras su exposición a este tipo de delitos se debe a la falta de controles y la pésima gestión al riesgo financiero. A continuación, se expondrán en resumen los casos más relevantes y conocidos a nivel mundial.

1. **Jérome Kerviel**, empleado del banco francés Société Générale, causó una pérdida de 6.170 millones de euros debido a transacciones especulativas ilícitas en el año 2008. Kerviel había estado operando de manera ilegal, anticipándose a la caída de los precios del mercado.

2. El **banco Bear Stearns** había quebrado tras realizar grandes inversiones en títulos hipotecarios de tipo subprime (hipotecas de alto riesgo). Estas hipotecas se otorgaban a personas con baja solvencia económica o ingresos inestables, lo que las convertía en un perfil de alto riesgo. Debido a este riesgo, los bancos compensaban la inversión con intereses elevados y la garantía de embargo de las propiedades hipotecadas en caso de impago. Así, se creó un círculo vicioso basado en préstamos cada vez más difíciles de pagar.

   Cuando los títulos hipotecarios perdieron su valor, el banco Bear Stearns quedó endeudado con más de 48,000 millones de dólares. La confianza en la entidad se desplomó hasta el punto de que tuvo que declararse en bancarrota.

3. **Lehman Brothers** se declaró en quiebra el 15 de septiembre de 2008, con un pasivo de 430.000 millones de dólares, lo que desató un efecto dominó a nivel global y culminó en la mayor crisis económica de la historia, conocida como la Gran Recesión. La entidad había realizado inversiones de alto riesgo en el sector inmobiliario, otorgando hipotecas subprime y una gran cantidad de créditos personales de difícil recuperación. Para 2007, el valor de Lehman Brothers en bolsa había caído un 95% respecto a su valor previo, lo que representaba pérdidas por 2.800 millones de dólares. La única opción para evitar la quiebra era que otra compañía la adquiriera, pero dicha compra nunca se concretó.

4. En 2011, la empresa financiera **MF Global** se declaró en quiebra después de que se revelara que había estado mezclando fondos propios con los de sus clientes para realizar transferencias y préstamos ilícitos. El monto defraudado ascendió a 36.000 millones de euros (Economista, 2019)

5. Tres banqueros de **Credit Suisse** fueron arrestados por conspirar en un esquema de préstamos en el que desviaron cientos de millones de dólares de la industria pesquera y de las defensas costeras de Mozambique, con el objetivo de sobornar a funcionarios del gobierno. El fraude del 2013 al 2016 alcanzó un total de 1.763 millones de dólares.

6. En julio de 2016, la policía de Argentina detuvo a **Hernán Arbizu**, ex vicepresidente de JP Morgan Chase. Arbizu había ocupado altos cargos en instituciones financieras internacionales, como Citibank, Bank Boston, Bank of America, UBS y Deutsche Bank. Durante su carrera, aprovechó su acceso a información privilegiada como datos confidenciales de clientes y transacciones para contactar potenciales clientes, lo que le permitió obtener jugosas comisiones.

   A pesar de haber ascendido a la vicepresidencia de JP Morgan Chase, Arbizu continuó operando en secreto, gestionando cuentas bancarias de clientes de los bancos donde había trabajado previamente. A través de estas cuentas, realizaba transferencias no autorizadas y facilitaba el lavado de dinero, enviando fondos a paraísos fiscales en el extranjero. De esta manera, aprovechaba su posición para realizar operaciones ilícitas y beneficiar a ciertos clientes de Argentina. (Pirani, 2024)

4.5 PRINCIPALES CASOS DE FRAUDES BANCARIOS EN HONDURAS.

En términos generales, se puede afirmar que el sistema financiero de Honduras es estable. Sin embargo, como cualquier sistema, no está exento de enfrentar crisis provocadas por fraudes bancarios. A lo largo de la historia, ha habido varios casos significativos que aún permanecen en la memoria colectiva de la población hondureña. A continuación, se presentarán los más relevantes.

1. **El Banco Corporativo (BANCORP), el Banco Hondureño de Crédito y Seguros (BANHCRESER) y Banco Capital** fueron fundados entre 1993 y 1994, lo que generó una sobre liquidez en el sistema bancario hondureño. Esta situación obligó a otros bancos a buscar aumentar su cartera de negocios mediante el otorgamiento de préstamos a los sectores productivos, sin antes verificar si los prestatarios contaban con la capacidad de pago necesaria.

   Esta crisis, conocida como la "fiebre crediticia", comenzó en 1996 y estuvo marcada por el sobreendeudamiento de los sectores productivos, especialmente del sector agropecuario. Se cree que la fiebre crediticia fue producto de la falta de supervisión y fiscalización por parte de los funcionarios públicos sobre las actividades financieras de los bancos, sus administradores y accionistas. Además, influyó la caída de los precios internacionales, lo que afectó la competitividad del sistema productivo en los mercados globales, el aumento de las tasas de interés reales y los daños provocados por el Huracán Mitch.

   En 2003, se arrestó a Víctor Bendeck, acusado por la Fiscalía General de la República de realizar “maniobras dolosas” que llevaron a la quiebra del Banco Corporativo (BANCORP). Se estima que al menos 30 banqueros utilizaron de forma ilegal 264 millones de dólares de los depósitos de los clientes para crear empresas personales y familiares, lo que resultó en la quiebra de los tres bancos mencionados, así como de cuatro financieras privadas. El gobierno solo garantizó el 70% de los depósitos de los bancos que quebraron. (El puso, 2017)

   Banco Capital tenía alrededor de 40,000 ahorrantes que habían depositado cerca de 730 millones de lempiras, de los cuales solo 230 millones estaban respaldados por el Fondo de Seguros de Depósitos (FOSEDE). Se cree que los principales responsables fueron Ivis y Fernández López, aunque no enfrentaron consecuencias penales. Además, se afirma que los socios del banco se habrían repartido unos 400 millones de lempiras (aproximadamente 23.5 millones de dólares) sin ninguna garantía, los cuales fueron transferidos como préstamos a otras empresas de su propiedad**.** (El pulso, 2020)

El Ministerio Público presentó una acusación criminal contra los directivos y administradores de **BANHCRESER.** Esta institución incurrió en irregularidades, incluyendo actos que podrían ser considerados como estafa y el manejo inapropiado de los fondos de disponibilidad inmediata depositados en el HSBC Bank, que ascendían a 3.7 millones de dólares. También se les acusó de otorgar créditos de manera irregular a empresas relacionadas mediante la apertura de sobregiros, excediendo los límites legales establecidos para operaciones con partes relacionadas. (El pulso, 2017)

2. En octubre de 2015, la Comisión Nacional de Bancos y Seguros (CNBS), el ente regulador, ordenó la liquidación forzosa del Banco Continental. Se estima que la institución realizó transacciones por más de 350 millones de lempiras (equivalentes a más de 15 millones de dólares) que no fueron aprobadas por el ente regulador. Además, se descubrió que el banco compró acciones en otra institución del sistema financiero. Aunque no se conocen todos los detalles, se subrayó que esta operación fue irregular, ya que se realizó después de que se iniciara la liquidación forzosa. (Negocios, 2015)

3. A principios de 2023, las oficinas de la Dirección Policial de Investigaciones (DPI) en San Pedro Sula, Santa Bárbara y Copán registraron entre seis y diez denuncias diarias por estafas bancarias, con montos que oscilan entre 15,000 y 190,000 lempiras. Estas estafas involucran a tres instituciones bancarias del país y se realizan mediante transacciones en línea, con fondos depositados en otros bancos. (La Prensa, 2023)

4. El 5 de septiembre de 2024, fueron detenidos cuatro ex empleados de un banco comercial, acusados de lavado de activos y estafa continua. Los implicados son Ayline Jemina Cruz Ortiz (ex empleada del banco y presunta cabecilla de la red de estafa), su pareja Félix Josué Durón, Delmer Jeovanny Cárdenas Garay (exempleado) y Miguel Darío Domínguez Garay (agente bancario).

   Los hechos fueron denunciados por la Gerencia de Cumplimiento de la institución donde laboraban, y ocurrieron durante los meses de abril y mayo del presente año. Las alertas se activaron cuando se detectaron transacciones atípicas realizadas desde una de las agencias

del banco, utilizando tarjetas de crédito o débito asociadas a cuentas de ahorro. El perjuicio financiero asciende a más de 11 millones de lempiras (11,260,759.39).

Una vez procesadas las transacciones, estas eran anuladas; sin embargo, los fondos eran acreditados a las cuentas particulares de los implicados, quienes inmediatamente realizaban retiros del dinero y lo entregaban a terceros. (Heraldo, 2024)

4.6 ESTADÍSTICAS GLOBALES SOBRE FRAUDES BANCARIOS

Según el informe sobre delitos financieros globales de NASDAQ 2024, el sistema financiero mundial sufrió pérdidas por estafas y fraudes bancarios que ascendieron a 485,600 millones de dólares en 2023. Sin embargo, el informe destaca que estas cifras podrían estar subestimadas, ya que muchos de estos delitos no son denunciados por las víctimas (GLEIF, 2024)

En respuesta a esta creciente amenaza, empresas como **BioCatch** han emprendido investigaciones para ofrecer soluciones innovadoras contra el fraude digital, el lavado de dinero y la suplantación de identidad. Un estudio realizado por BioCatch sobre tendencias de fraude en Europa reveló varios hallazgos clave: (BioCatch, 2024)

1. El 75% de los casos de fraude informados por los clientes europeos de BioCatch ocurrieron a través de dispositivos móviles.
2. Los incidentes de dispositivos robados aumentaron un 43% en la región, con el Reino Unido, España y Portugal siendo los países más afectados.

3. La herramienta de detección de cuentas "mulas" de BioCatch identificó más de 10,000 cuentas de este tipo entre los clientes europeos.
4. Las estafas telefónicas (Vishing) disminuyeron un 25% en el Reino Unido, mientras que las "capturas de cuentas" (ATO, por sus siglas en inglés) aumentaron en un 13%.

En América Latina, la empresa **Appgate** reportó que en 2023 se registraron un promedio de 45 alertas diarias de fraude, frente a las 32 alertas diarias reportadas en Norteamérica. (Idárraga, 2024)

En cuanto a ciberseguridad, el **Fondo Monetario Internacional (FMI)**, en su informe sobre Estabilidad Financiera Mundial 2024, destacó que entre 2004 y 2023, el 20% de los incidentes cibernéticos registrados afectaron al sector financiero, con pérdidas cercanas a 12,000 millones de dólares. De esta cifra, 2,500 millones de dólares corresponden a incidentes ocurridos desde 2020, lo que subraya la creciente amenaza a las infraestructuras financieras.
A pesar de la magnitud de los fraudes, solo el 38% de los bancos en América Latina invierten en ciberseguridad e inteligencia artificial, según el Estudio Latinoamericano de Banca Digital de Infocorp Surveys. (Idárraga, 2024)

Las estafas continúan evolucionando y, según la **Interpol**, las tendencias de fraude para 2024 varían según el continente. En **África**, una de las modalidades más frecuentes es la suplantación de identidad mediante correos electrónicos, junto con el creciente uso del fraude conocido como **"pig butchering"**, en el que los delincuentes manipulan las emociones de las víctimas para que inviertan en proyectos ficticios.

En **América**, las estafas más comunes incluyen la **usurpación de identidad**, fraudes emocionales, estafas relacionadas con asistencia técnica y pagos adelantados por servicios que nunca se prestan.

En **Asia**, el "pig butchering" también está en aumento, además del robo de información personal a través de llamadas fraudulentas de supuestos agentes del orden o de instituciones bancarias. Finalmente, en **Europa**, las estafas más comunes son el **phishing** y otros fraudes a través de internet, en los que las víctimas son cuidadosamente seleccionadas, lo que complica aún más la detección de los engaños. (Interpol, 2024)

En conclusión, las estafas y fraudes en el ámbito financiero están en constante crecimiento, afectando a diferentes regiones del mundo de manera distinta. La falta de inversión adecuada en ciberseguridad y la subestimación de los riesgos por parte de muchas instituciones financieras son factores que agravan esta situación. La implementación de soluciones innovadoras como las que ofrece BioCatch es esencial para combatir estas amenazas.

4.7 ESTADÍSTICAS SOBRE FRAUDES BANCARIOS EN HONDURAS.

Según el "Reporte de Inclusión Financiera 2024" presentado por la Comisión Nacional de Bancos y Seguros (CNBS) en el 2023 se registró un incremento del 50% en los reclamos de personas naturales ante las instituciones supervisadas. La mayoría de estos reclamos fueron de la categoría de Phishing, la cual tuvo un aumento en un 343.8%, representando el 80% de los casos adicionales. Como se puede observar en el **Anexo 1 Tabla de la evolución de los reclamos presentados por los usuarios financieros antes las instituciones supervisadas.** (CNBS, 2024)

Debido a la Pandemia del COVID-19 y su confinamiento que se experimentó a nivel mundial, las personas, empresas e instituciones supervisadas se vieron obligadas a implementar métodos digitales para la realización de sus servicios, productos y pagos. Provocando el incremento de los casos de phishing por medio de estos en donde los ciberdelicuentes se aprovechan de la falta de conocimiento por parte de algunos usuarios o las debilidades presentadas en ciertas plataformas.

El Ministerio Público en las oficinas de la Dirección Policial de Investigación (DPI) en el mes de marzo del 2023 recibió 110 denuncias por delitos de financieros e informáticos. Tales delitos fueron por acceso no autorizado a sistemas informáticos, en donde, se realizó un cambio de claves de las cuentas bancarias y el dinero fue transferido a otras cuentas bancarias de la misma agencia financiera.

Los montos de los afectados fueron desde los 10 mil a un millón de lempiras, su información personal fue sustraída por los malhechores de forma voluntaria por los medios de cuentas bancarias falsas, correos electrónicos, llamadas o mensajes por redes sociales. También se recibieron denuncias por los delitos de suplantación de identidad, que es cuando una persona se hace pasar por otra para hacer fraude o cometer estafas. (Publico, 2023)

Cabe destacar que, durante el mismo mes de marzo del 2023, la CNBS informo al diario El Tiempo que se habían registrado alrededor de 300 reclamos por fraudes a cuentas bancarias en los diferentes bancos del país. Provocando una gran consternación a la institución supervisora

sobre las medidas de seguridad de los bancos del sistema financiero, ya que dichos fraudes fueron por hackeo de la información o el uso de sus cuentas bancarias. (Amador, 2023)

En el año 2024 también se ha visto una gran participación en estas actividades delictivas, según un informe de la Gerencia de Protección al Usuario Financiero de la CNBS, los casos de fraudes y operaciones sospechosas con tarjetas de crédito, de débito y financiamiento reporta un incremento del 50%. (Rodriguez, 2024)

Y de acuerdo con el Ministerio Publico entre el 2023 y julio del 2024 más de 150 personas han presentado denuncias por ser víctimas de estafas a través de las distintas redes sociales siendo las más usada Facebook, Messenger y el correo electrónico. (Giron, 2024)

En el marco de la actual investigación, el Banco Central de Honduras (BCH) emitió un comunicado (**ver Anexo 2. Comunicado BCH 11/11/2024**) en el que hace un llamado a la población, tanto a nivel nacional como internacional, ante el surgimiento de una nueva plataforma denominada 'Financing Latam'. Esta plataforma circula a través de las redes sociales, como Facebook y WhatsApp, y presenta un video en el que se solicita a las personas realizar pequeñas inversiones a cambio de grandes ganancias. En este sentido, el BCH reitera que no ofrece este tipo de inversiones ni solicita información personal o financiera.

Asimismo, se recuerda a los usuarios que los únicos canales de comunicación oficiales del Banco son su portal digital y sus redes sociales verificadas.

4.8 EL ROL Y LAS RESPONSABILIDAD DE LAS INSTITUCIONES BANCARIAS

Con el fin de mitigar dicho riesgo, la CNBS emitió el **Anexo 3: Comunicado de la CNBS 24/03/2023** el cual presenta los lineamientos Mínimos con los que deben contar las Instituciones Supervisadas para prevenir y mitigar la ocurrencia de fraudes y estafas cibernéticas en contra del usuario financiero.

La CNBS les exige a sus entidades supervisadas

1. Una estrategia de mitigación de fraudes cibernéticos. Dicha estrategia debe minimizar los

riesgos de fraude cibernéticos por medio de los canales digitales que ponen a disposición de sus usuarios financieros, realizada de manera conjunta con las políticas de seguridad de la institución, unidades de negocio y las funciones de vigilancia alineados con las políticas con las políticas de seguridad de la institución. Su principal objetivo es determinar si los controles implementados son suficientes para mitigar tipologías de fraude.

2. Educación Financiera: Las instituciones bancarias deben informar y concientizar a los usuarios sobre la prevención de fraudes y estafas cibernéticas mediante las campañas masivas de educación financiera. Conteniendo los elementos de:
    a. Riesgos asociados a los productos y servicios por medio de canales digitales
    b. Prácticas de ingeniería social que utilizan los estafadores para obtener información confidencial
    c. Buenas prácticas de protección de sus credenciales de usuario
    d. Concientizar a los usuarios que las entidades bancarias nunca solicitaran su usuario, clave u OTP.
    e. Protección del correo electrónico personal registrado para hacer uso de los canales digitales, doble factor de autentificación y uso de contraseñas robustas.
    f. Detección de un ataque de secuestro de número telefónico (SIM Swap)
    g. Promover el uso de la aplicación oficial
    h. Orientar a los usuarios a reconocer una URL oficial contra una fraudulenta

3. La institución bancaria debe de contar con mecanismos que les permita identificar nuevas tipologías de fraudes y estafas cibernéticas que esté ocurriendo en la región o en el país.
4. Las instituciones bancarias tienen la responsabilidad de contar con controles preventivos, que puedan detectar y correctivas para que puedan proteger las cuentas de los usuarios. Tales controles deben identificar y responder ante transacciones sospechosas o atípicas.
5. Igualmente, deben contar con un análisis de riesgo en sus mecanismos de autogestiones en canales digitales para los cambios de tokens, creación de usuarios, cambio de claves, bloqueo de cuentas en donde se incluya por lo menos los siguientes elementos:
    a. Un servicio que analice el canal digital
    b. Mecanismos que garanticen al cliente la autenticidad que la comunicación proviene de la institución bancaria.

c. Cultura de contraseñas robustas
d. Mecanismos para la protección de marca
e. Tiempos de expiración por inactividad en las sesiones
f. Doble factor de autenticación
g. Límites de intentos de inicio de sesión
h. Límite de tiempo para la validación de la OTP (One time password)
i. Limites diferenciados para transferencias a terceros ACH, LBTR, y otros.

6. Reporte de eventos: Estas instituciones deberán de reportar a la Comisión sobre los incidentes de fraude cibernético en un plazo de veinticuatro horas luego de haber identificado el incidente, brindando información del usuario, así como la descripción del incidente.
7. Notificación y reclamo de transacciones electrónicas no autorizadas: El usuario financiero debe notificar a la entidad bancaria sobre la ocurrencia de la transacción electrónica no autorizada en un plazo de cuarenta y ocho horas a partir de la fecha que se ha enterado.
8. Denuncia ante las autoridades competentes: las entidades bancarias deben requerir a los titulares de cuentas afectadas que se aboquen a las autoridades judiciales correspondientes para que presenten su denuncia sobre las operaciones fraudulentas.

4.9 MARCO LEGAL DE HONDURAS

En Honduras, las consecuencias por delitos de fraude o estafa están reguladas por el **Código Penal**, específicamente en el **artículo 365**. En el cual se establece que "para la determinación de la pena de estos delitos se debe atender el importe de lo defraudado, la pérdida económica causada al perjudicado, las relaciones entre este y el defraudador, los medios empleados por el reo y cualesquiera otras circunstancias similares que sirvan para valorar la gravedad de la infracción". (Legislativo, 2019)

De acuerdo con este artículo, el delito de estafa será castigado con una pena de prisión de dos a cuatro años si el valor defraudado supera los cinco mil lempiras.

Además, el nuevo **Código Penal** de Honduras también establece sanciones para los delitos informáticos, específicamente en el **Título XXII: Seguridad de las redes y sistemas**

informáticos. El **artículo 398**, relacionado con el **Acceso no autorizado a sistemas informáticos**, especifica que debe de ser castigado de pena de prisión de seis a dieciochos meses o multa de cien a doscientos días quien, vulnerando las medidas de seguridad establecidas para impedirlo y accede sin autorización a todo en parte de un sistema informático.

Igualmente, en el **artículo 401**, relacionado con la **Suplantación de identidad** determina que debe ser castigado con la pena de prisión de seis meses a un año o multa de cien a trescientos días, quien con anima defraudatorio y a través de las tecnologías de la información y la comunicación, suplanta la identidad de una persona natural o jurídica.

Honduras está demostrando un esfuerzo por adaptarse a las nuevas tácticas empleadas por los delincuentes para llevar a cabo fraudes bancarios y delitos informáticos. A través de la actualización de su **Código Penal**, el país ha comenzado a incorporar medidas más rigurosas para sancionar tanto las estafas tradicionales como los delitos que involucran el uso de tecnología, como el acceso no autorizado a sistemas informáticos.

Estos avances legislativos reflejan un reconocimiento de la creciente sofisticación de los fraudes, que hoy día no solo afectan a los individuos, sino que también ponen en riesgo la seguridad de las instituciones financieras y la estabilidad económica.

4.10 EDUCACIÓN FINANCIERA EN HONDURAS

Entre 2020 y 2023, se realizaron un total de 1,436 capacitaciones en educación financiera, de las cuales 1,040 correspondieron a webinars y 396 a formaciones presenciales, que incluyeron talleres, charlas y simuladores sobre diversos temas de relevancia. Estas capacitaciones beneficiaron a 80,182 personas, de las cuales el 69% (49,737) fueron mujeres y el 31% (30,445) fueron hombres. En 2023, predominó la modalidad presencial, con 385 capacitaciones frente a 217 webinars. (CNBS, Reporte de inclusión Financiera 2024, 2024)

A nivel departamental, Francisco Morazán fue el departamento con mayor número de capacitaciones, alcanzando 338 (56.3% del total), seguido por Cortés con 79 (13.1%) y Valle con 43 (7.1%). **Ver Anexo 4 Número de capacitaciones impartidas en materia de Educación Financiera a nivel departamental 2023.**

A través del Aula Virtual de la CNBS, se ofrecieron 12 cursos en línea entre 2020 y 2023, alcanzando un total de 1,507 participantes. De ellos, el 59% (883) fueron mujeres y el 41% (624) hombres. **Ver Anexo 5 Número de capacitaciones impartidas en el Aula Virtual por sexo durante el periodo de 2020-2023.**

La CNBS también organiza eventos masivos de educación financiera, entre los que se destacan:

- **Semana Mundial del Dinero (Global Money Week):** Dirigida especialmente a niños y jóvenes.
- **Día Mundial del Ahorro:** Con el objetivo de sensibilizar a la población sobre la importancia del ahorro.
- **Semana de Educación Financiera (SEF):** Un espacio para proporcionar a niños, jóvenes y adultos las herramientas necesarias para hacer un uso adecuado y responsable de los productos y servicios financieros.

En 2023, los eventos masivos organizaron los siguientes números de participantes:

- **Global Money Week:** 14,470 participantes.
- **Día Mundial del Ahorro:** 66,132 participantes.
- **Semana de Educación Financiera:** 7,953 participantes.

Ver Anexo 6 Eventos de Educación Financiera realizada por la CNBS (2021-2023)

Hasta noviembre de 2024, según las estadísticas de la CNBS, se han impartido 585 capacitaciones en educación financiera. De ellas, el 60% (14,863) de los participantes fueron mujeres, incluyendo niñas y jóvenes, mientras que el 40% (9,906) correspondió a hombres, incluyendo niños, jóvenes y adultos. De las capacitaciones realizadas en 2024, 450 fueron presenciales y 135 se llevaron a cabo a través del Aula Virtual. (CNBS, CNBS, 2024)**.**
A nivel departamental, las capacitaciones en 2024 se distribuyeron de la siguiente forma: Francisco Morazán lideró con 183 capacitaciones (31.3% del total), seguido por Cortés con 96 (16.4%) y Comayagua con 74 (12.7%). **Ver Anexo 7 Número de capacitaciones impartidas en materia de Educación Financiera a nivel departamental 2024 hasta noviembre.**

CAPÍTULO V. METODOLOGÍA / PROCESO

La investigación adopta un enfoque metodológico mixto, integrando tanto técnicas cualitativas como cuantitativas para un análisis integral. Se emplearán las siguientes herramientas:

- **Revisión de literatura:** Se llevará a cabo un análisis exhaustivo de bibliografía especializada en el área bancaria, así como de boletines informativos que aborden el impacto del fraude bancario y como la educación financiera ayuda a prevenirlo.
- **Análisis de datos secundarios:** Se examinarán estadísticas oficiales proporcionadas por la Comisión Nacional de Bancos y Seguros (CNBS) y otras fuentes pertinentes que puedan ofrecer información relevante sobre el tema de estudio.
- **Encuestas:** Se realizarán encuestas a usuarios activos de la banca hondureña, y se llevará a cabo un conjunto de investigaciones referentes al impacto de como el fraude afecta el sistema bancario.

5.1 ENFOQUE Y MÉTODOS

5.1.1 ENFOQUE

El enfoque principal de esta investigación es enfoque mixto, ya que, al analizar el impacto del fraude bancario en las instituciones financieras de Honduras, así como las consecuencias que este fenómeno ha tenido para los usuarios de los servicios bancarios. Se pretende examinar cómo el fraude ha afectado tanto la seguridad y estabilidad de las entidades bancarias como la confianza de los clientes en el sistema financiero. Esta investigación abordará diversos tipos de fraudes que han prevalecido en el contexto bancario hondureño, tales como el robo de dinero, la suplantación de identidad, la clonación de tarjetas bancarias y el robo de información personal y financiera, los cuales han causado pérdidas económicas significativas tanto para los usuarios como para las instituciones. Además, se analizarán las vulnerabilidades en los sistemas de seguridad de las entidades bancarias y las prácticas fraudulentas más comunes utilizadas por los delincuentes, con el fin de entender mejor cómo operan estos fraudes y qué medidas se han tomado para prevenirlos.

- **Enfoque Mixto:** Dado que el fraude bancario involucra tanto aspectos cuantificables (por ejemplo, las pérdidas económicas y la frecuencia de los fraudes) como factores cualitativos (como las percepciones de los usuarios o las prácticas de seguridad), el enfoque metodológico será mixto. Este permitirá combinar el análisis numérico con la interpretación de experiencias y opiniones, brindando una comprensión más completa del fenómeno.
- **Enfoque Cuantitativo:** El enfoque cuantitativo se utilizará para analizar los datos estadísticos relacionados con la incidencia del fraude bancario en Honduras, a través de indicadores como el número de casos reportados, las pérdidas económicas generadas, las variaciones en las cifras de fraude a lo largo del tiempo, entre otros.
- **Enfoque Cualitativo:** El enfoque cualitativo permitirá profundizar en las experiencias subjetivas y las percepciones de los usuarios, empleados bancarios y expertos en seguridad, proporcionando información más detallada sobre las causas y las consecuencias del fraude bancario.

5.1.2 MÉTODOS

Para realizar un análisis preciso del impacto del fraude bancario en el sistema hondureño, resulta fundamental seleccionar una muestra representativa de la población objetivo, asegurando que los resultados obtenidos reflejen fielmente la realidad del sector financiero en el país. El objetivo de esta investigación es examinar los efectos del fraude bancario en el sistema financiero de Honduras, incluyendo las consecuencias económicas y emocionales en los usuarios afectados, y el grado de confianza que estos mantienen en el sistema bancario.

Para recoger la información necesaria, se aplicarán encuestas **(Ver Anexo 8. Encuesta aplicada a usuarios actuales de la banca en línea)** a una muestra diversa de usuarios de servicios bancarios, junto con entrevistas a expertos del sector y análisis de datos estadísticos de entidades regulatorias.

5.2 POBLACIÓN Y MUESTRA

5.2.1 POBLACIÓN

El fraude en el sistema bancario hondureño ha tenido un impacto significativo, afectando tanto a los usuarios, como a la credibilidad de las instituciones financieras. En respuesta, el gobierno de la República, a través de su ente regulador, la Comisión Nacional de Bancos y Seguros (CNBS), implementó un programa de educación financiera en 2014. Este programa ha tenido un impacto positivo en los usuarios, quienes han adquirido conocimientos y habilidades para gestionar mejor sus ingresos y tomar decisiones financieras.

Instituciones Bancarias: Los principales bancos considerando la cantidad de activos y sucursales, se priorizan las instituciones con mayor presencia en el país, ya que suelen tener un impacto significativo en el sistema bancario y un mayor número de transacciones.

- **Usuarios Afectados:** Los clientes de las instituciones bancarias, individual como empresas, pueden ser afectados por los fraudes en diversas formas: perdidas de capital, robo de identidad.
- **Empleados del Sistema Bancario:** El personal que trabaja en las areas claves de la institución, auditoria, tecnología, atención al cliente, los cuales desempeñan un papel fundamental en detectar, prevenir, y gestionar los fraudes.
- **El ente regulador:** El organismo que supervisa y regula el sistema financiero es la Comisión Nacional de Bancos y Seguros (CNBS) la cual establece directrices, normativas, promueven medidas para evitar el fraude, protegiendo al usuario, y logrando estabilidad del sistema bancario.

Se utilizaron datos del Instituto Nacional de Estadística (INE), los cuales reportan que para el año 2023, la población total era de 1,132,551 personas. De este total, 821,099 corresponden a la población económicamente activa, lo que representa el 72.5%. Asimismo, se consideró el acceso a internet, según datos del sector de telecomunicaciones proporcionados por CONATEL. Al cierre del año 2023, se reportaron 7,921,347 conexiones a internet en Honduras.

Tomando en cuenta la densidad poblacional del 11.78% correspondiente a Francisco Morazán, se estima que aproximadamente 933,135 personas en esta región tienen acceso al servicio de internet, lo que equivale a 10 de cada 100 hondureños.

5.2.2 MUESTRA

Para analizar con precisión el impacto del fraude en el sector bancario en Honduras, es fundamental elegir una muestra representativa de la población objetivo.

- **Tamaño de la muestra**: Debe ser lo suficientemente grande para asegurar resultados estadísticamente fiables, pero lo bastante manejable para facilitar la recolección y el análisis de la información proporcionada por los usuarios de la banca en línea.

Para esta investigación, se tomó en consideración la población usuaria de la banca en línea y los habitantes potenciales del distrito central. La muestra será determinada a través de encuestas aplicadas a hombres y mujeres económicamente activos, con edades entre 18 y 60 años en adelante, residentes en el distrito central.

Para el cálculo del tamaño de la muestra se hace uso de la siguiente formula:

n=(z^2(p*q))/(e^2+(z^2 (p*q))/N)

Donde:

N= Total de la población = 933,135
z= Nivel de confianza deseado = 95% (1.95)
p= Margen de error= 5% (0.5)
q =1-p (1-0.5=0.5)
e= error de la muestra 0.05
Desarrollo:
n=((1.95) ^2(0.5*0.5))/(〖(0.05)〗^2+((1.95)^2 (0.5*0.5))/933,135)
n=385

- **Método de muestreo**: El método de muestreo debe ser aleatorio para garantizar que todos los usuarios de la banca en línea tengan la misma oportunidad de participar, proporcionando respuestas confiables que permitan realizar un análisis preciso.

5.3 UNIDAD DE ANÁLISIS Y RESPUESTA

5.3.1 UNIDAD DE ANÁLISIS

Los datos recopilados se analizarán empleando métodos estadísticos adecuados, tomando en cuenta las variables de segmentación pertinentes. Este análisis buscará identificar los principales impactos del fraude bancario, proporcionando una visión detallada de sus efectos en distintos segmentos de la población.

5.3.2 UNIDAD DE RESPUESTA

La unidad de análisis de esta investigación se establecerá a partir de las respuestas obtenidas de las encuestas dirigidas a usuarios de la banca en línea del sistema bancario en Honduras.
Al obtener datos precisos sobre las experiencias, percepciones y preocupaciones de los usuarios respecto al fraude bancario, se identificarán patrones de uso, conductas recurrentes que podrían estar relacionadas con el fraude, al mismo tiempo se medirá el nivel de confianza de los usuarios de la Plataforma banca en línea.

5.4 TÉCNICAS E INSTRUMENTOS APLICADOS

Los recursos empleados para la recopilación de datos se componen de cuestionarios digitales creados en la plataforma Office Forms. Esta encuesta estará accesible mediante un vínculo compartido, facilitando a los usuarios su acceso y respuesta de forma fácil. **Ver Anexo 8. Encuesta aplicada a usuarios actuales de la banca en línea.**

El propósito principal de las encuestas es recolectar datos acerca de si los usuarios de la banca en línea han sufrido fraudes y si están al tanto de los procedimientos existentes para evitar tales sucesos. Además, es crucial elegir herramientas apropiadas para la población objetivo, garantizando la recolección de datos pertinentes y valiosos para el análisis subsiguiente.

Para recolectar la información aplicará la encuesta a:

- Hombres y mujeres.
- Edades de 18-60 años en adelante
- Población con acceso a internet.
- Residentes en el distrito central
- La encuesta se aplicó de manera online durante el mes de noviembre del año 2024

5.5 FUENTES DE INFORMACIÓN

Las fuentes de información son fundamentales para la recopilación de datos y el análisis de las investigaciones. Estas fuentes pueden ser primarias, como entrevistas, documentos originales o encuestas, o secundarias, como estudios previos e informes. Se debe elegir fuentes confiables y relevantes para asegurar la precisión y veracidad en la investigación y en su análisis.

5.5.1. Fuentes Primarias

Las fuentes primarias son objetos, imágenes, documentos o registros creados durante el periodo histórico que se estudia, lo que les confiere un carácter auténtico y directo. Estas fuentes ofrecen una perspectiva personal e inmediata sobre eventos, procesos o contextos específicos, convirtiéndose en una herramienta invaluable para los investigadores.

Las fuentes primarias utilizadas en esta investigación son las siguientes:

- Encuestas

5.5.2. Fuentes Secundarias

Las fuentes secundarias se elaboran con el propósito de interpretar, analizar, evaluar o resumir objetos, documentos o eventos históricos. Estas obras ofrecen una perspectiva reflexiva y crítica que complementa el estudio de las fuentes primarias, facilitando una comprensión más amplia y contextualizada de los hechos históricos.

Las fuentes secundarias utilizadas en esta investigación son las siguientes:

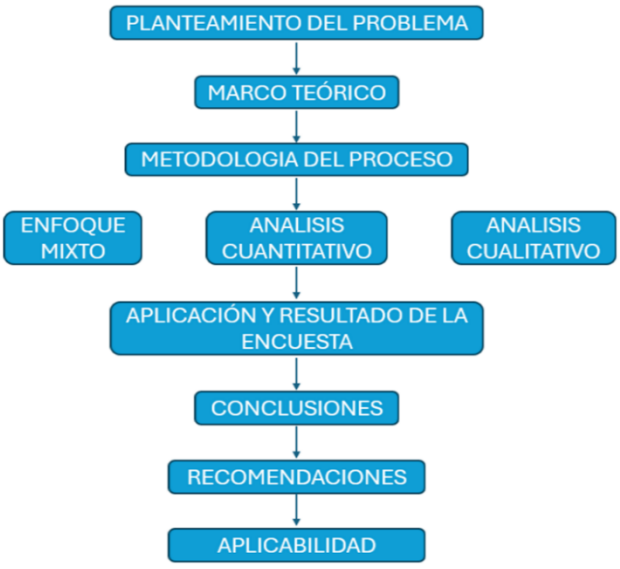
- Resolución No.247/23-03-2023 (www.cnbs.gob.hn)
- Comisión Nacional de Bancos y Seguros (CNBS): https://www.cnbs.gob.hn/
- Ministerio Publico: https://www.mp.hn/
- Banco Central de Honduras: https://www.bch.hn/
- Artículos y revistas digitales

5.6 CRONOLOGÍA DE TRABAJO

La cronología de trabajo es esencial para organizar y planificar una investigación, estableciendo un marco temporal para cada fase del proceso. Ayuda a gestionar el tiempo y los recursos de manera eficiente, asegura el cumplimiento de plazos y permite ajustar la planificación en caso de imprevistos, garantizando el éxito en la ejecución de la investigación. Para facilitar la comprensión del proceso de la investigación, a continuación, se presenta un diagrama del mismo, seguida de la cronología detallada del trabajo realizado.

1.1.1. Proceso de Investigación

Ilustración 1Proceso de Investigación



Fuente: Creación Propia

En la ilustración 1 se presenta la cronología del proceso llevado a cabo en la investigación, que incluyó varias etapas clave: el planteamiento del problema, la construcción del marco teórico, el diseño y aplicación de la metodología, la implementación de la encuesta, y, finalmente, la formulación de conclusiones y recomendaciones. Este esquema refleja el orden y la estructura seguidos para la elaboración de la investigación.

Ilustración 2 Cronología de la investigación

Actividades	TIEMPO TRANSCURRIDO											
	OCTUBRE				NOVIEMBRE				DICIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4
PLANTEAMIENTO DEL PROBLEMA												
MARCO TEORICO												
METOLOGIA DEL PROCESO												
APLICACIÓN Y RESULTADOS DE LA ENCUESTA												
CONCLUSIONES												
RECOMENDACIONES												
APLICABILIDAD												

Fuente: Creación Propia

En la ilustración 2 se detalla el avance realizado del proyecto de investigación corresponde a las 10 semanas, se observa que tanto el planteamiento del problema como el marco teórico se modificaron durante este periodo. La metodología se desarrolló en un lapso de 7 semanas, mientras que la aplicación y el análisis de los resultados de la encuesta se realizaron en 5 semanas. Este proceso permitió avanzar en las conclusiones, recomendaciones y la aplicabilidad en el mismo período de tiempo.

CAPÍTULO VI. RESULTADOS Y ANÁLISIS

A continuación, se analizan los resultados del impacto del fraude en el sistema bancario en Tegucigalpa, en los usuarios de la banca en línea, destacando las vulnerabilidades detectadas, a través de las encuestas, así mismo las consecuencias, y las medidas implementadas por la institución bancaria para mitigar el problema.

6.1 Encuestas realizadas a los usuarios de banca en línea, y la percepción que tienen frente al fraude en el sistema bancario en Tegucigalpa.

Pregunta No. 1 Género

Tabla No. 1

GÉNERO	CANTIDAD
Femenino	**246**
Masculino	**142**
Total	**388**

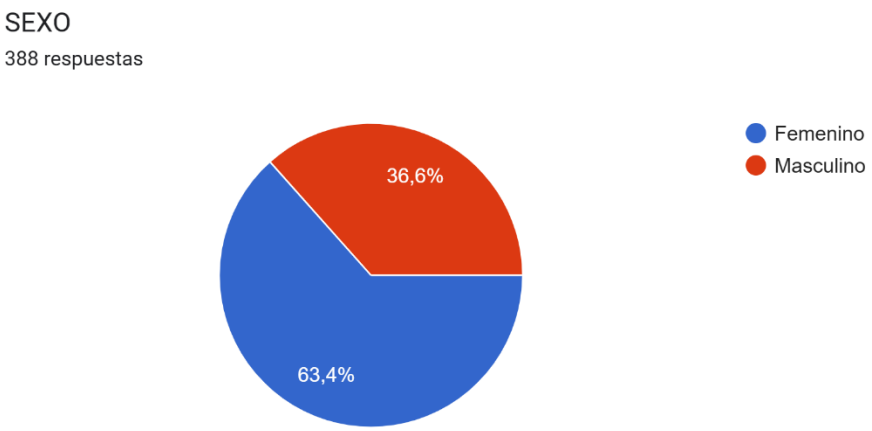


Gráfico 1 Sexo

La encuesta fue aplicada a una muestra total de 388 personas, de las cuales 246 son mujeres y 142 son hombres. Como se observa en el Gráfico 1, el 63.4% de los encuestados corresponde al género femenino, mientras que el 36.6% pertenece al género masculino.

Esto evidencia una predominancia del género femenino en las respuestas obtenidas a través del instrumento aplicado.

Además, los datos muestran una mayor participación de mujeres en comparación con hombres. Este resultado sugiere que, dentro de esta investigación, un porcentaje significativamente más alto de mujeres ha reportado haber sido víctimas de fraude en el sistema bancario.

Pregunta No. 2 Edad

Tabla No. 2

GÉNERO	CANTIDAD
18-24	60
25-30	69
31-36	67
37-45	71
46-50	50
51-60	31
60 años en adelante	40
Total	388

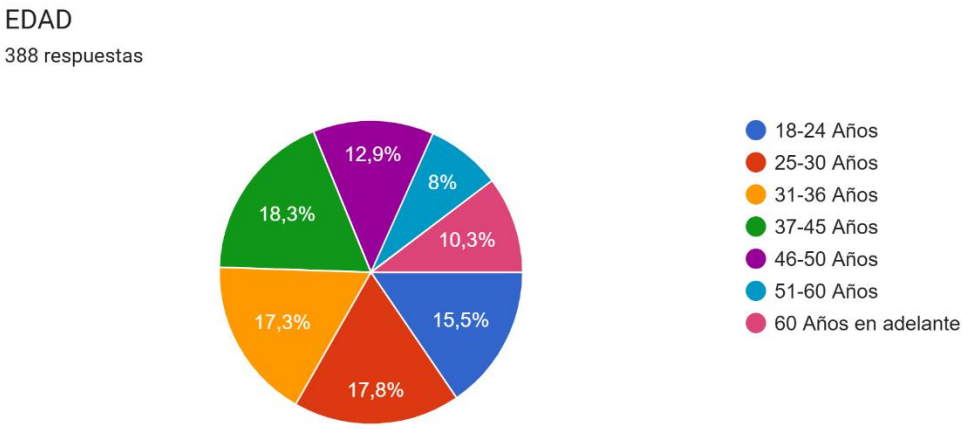


Gráfico 2 Edad

De las personas encuestadas, la distribución por rangos de edad se detalla a continuación:

- **37-45** años: 71 personas, lo que representa el 18.3% de la muestra. siendo el rango con

mayor participación.

- **25-30** años: 69 personas, equivalente al 17.8%.
- **31-36** años: 67 personas, lo que representa el 17.3%.
- **18-24** años: 60 personas, correspondientes al 15.5%.
- **46-50** años: 50 personas, lo que equivale al 12.9%.
- **60 años en adelante**: 40 personas, lo que representa el 10.3%.
- **51-60** años: 31 personas, correspondientes al 8% de la muestra.

Pregunta No. 3 ¿Usted utiliza banca en línea?

Tabla No. 3

¿Usted utiliza banca en línea?	Cantidad
Afirmativo	319
Negativo	69
Total	**388**

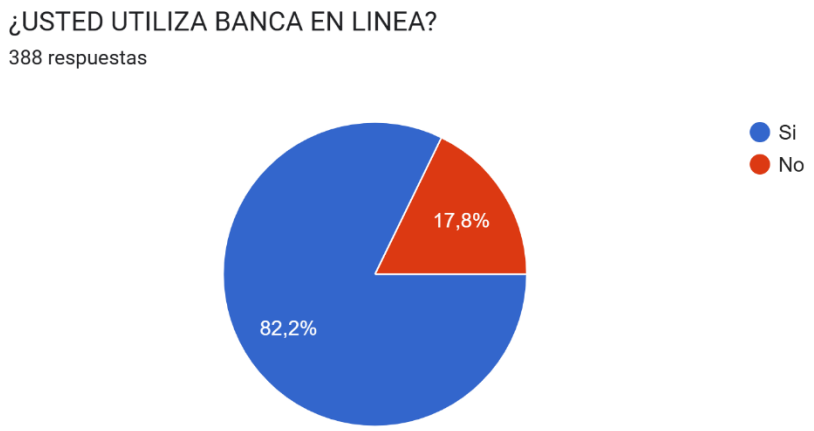


Gráfico 3 ¿Usted utiliza banca en linea?

De las 388 personas encuestadas, 319 utilizan banca en línea**,** lo que representa el **82.2%** de la muestra, indicando una alta adopción de esta modalidad entre los participantes. En contraste, 69 personas no utilizan la banca en línea, lo que corresponde al **17.8%**, evidenciando una menor proporción de usuarios que aún no han adoptado esta tecnología.

Pregunta No. 4 ¿Alguna vez ha sido víctima de fraude bancario o ha experimentado actividad sospechosa en sus cuentas?

Tabla No. 4

¿Alguna vez ha sido víctima de fraude bancario o ha experimentado actividad sospechosa en sus cuentas?	Cantidad
Afirmativo	204
Negativo	115
Total	**319**

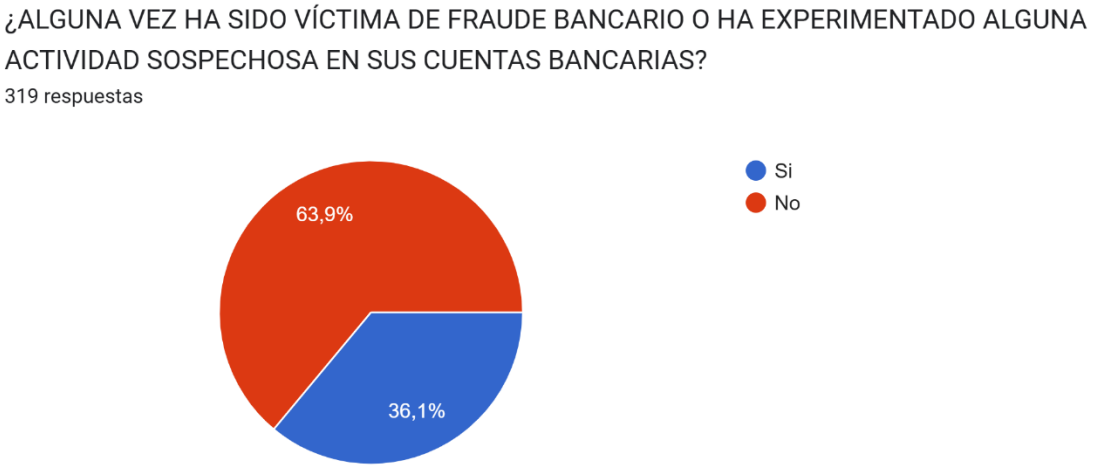


Gráfico 4 ¿Alguna vez ha sido víctima de fraude bancario o ha experimentado alguna actividad sospechosa en sus cuentas bancarias?

De las 319 personas encuestadas, 204 respondieron que no fueron víctimas directas de fraude, pero sí detectaron actividad sospechosa en sus cuentas. Por otro lado, 115 personas indicaron haber sido víctimas de fraude, lo que resalta la preocupación por la seguridad en línea y la posibilidad de que muchas personas hayan experimentado situaciones de riesgo.

Pregunta No. 5 ¿Qué acciones tomó la Institución bancaria para resolver el caso del fraude?

Tabla No. 5

¿Qué acciones tomó la Institución bancaria para resolver el caso del fraude?	Cantidad
Detección y Notificación Inmediata	40
Congelación de la Cuenta Afectada	59
Investigación Interna	59
Llenar formulario de reclamación	57
Reembolso de los fondos	56
Pasar el caso al ente regulador CNBS	25
Total	**115**

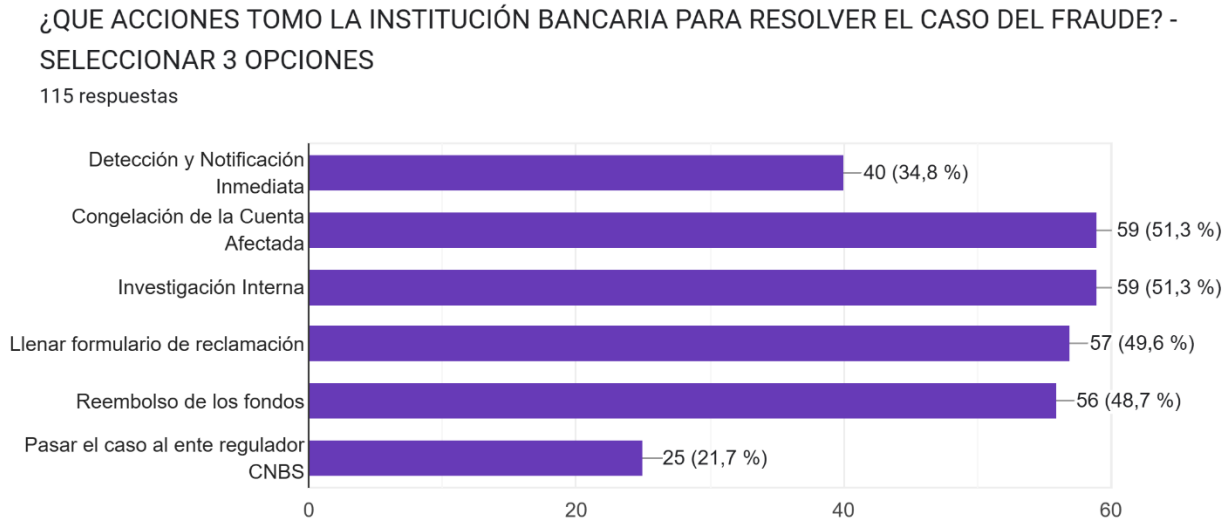


Gráfico 5¿Qué acciones tomo la institución bancaria para resolver el caso del fraude?

- **Detección y Notificación Inmediata (34,8%):** Según los usuarios de la banca en línea, la principal acción adoptada por las instituciones bancarias fue el detectar la actividad inusual en sus cuentas**.**
- **Congelación de la Cuenta Afectada (51,3%)** e **Investigación Interna (51,3%:** Según **l**a muestra los encuestados afirman que la institución bancaria les congelo la cuenta bancaria y

procedió con la investigación interna que esto representa el 51.3%

- **Llenar Formulario de Reclamación (49,6%):** Una gran proporción de los encuestados indicaron que llenaron el formulario de reclamación, lo que nos indica que están siguiendo con los procedimientos para gestionar los casos de fraude.
- **Reembolso de los Fondos (48,7%):** Nos deja evidenciado a través de la encuesta que las instituciones han reembolsado los fondos perdidos a los usuarios, lo cual ha ayudado a la institución a fortalecer la confianza y credibilidad.
- **Pasar el caso al ente regulador (21,7**%): Podemos observar que los casos no resueltos por la institución bancaria fueron escalados al ente regulador, la Comisión Nacional de Bancos y Seguros. Esto se refleja en la encuesta, lo que sugiere que el fraude podría tener implicaciones más complejas que requieren la intervención de un regulador externo para garantizar una resolución adecuada.

Pregunta No. 6 ¿Cuál de los bancos en el sistema hondureño utiliza con mayor regularidad?

Tabla No. 6

Instituciones Bancarias	Cantidad
Bac	47
Banco Atlántida	25
Ficohsa	22
Banco de Occidente	12
Davivienda	3
Banco del País	4
Lafise	1
Banco Cuscatlán	1
Total	**115**

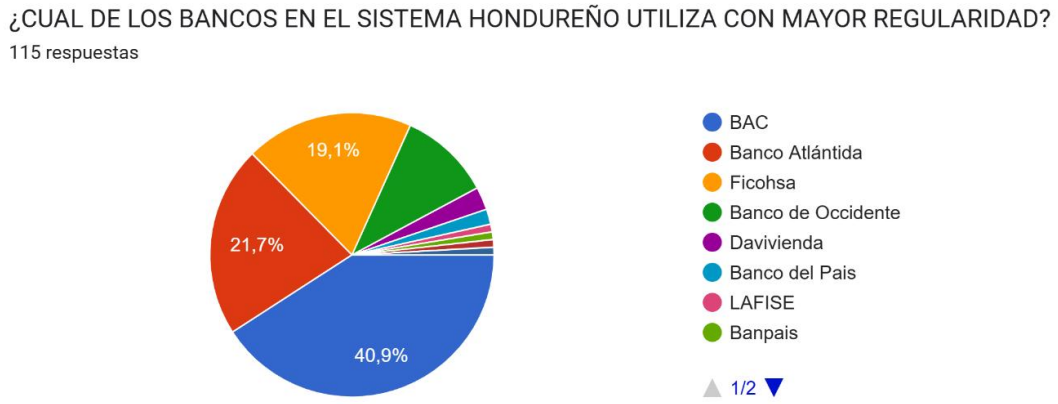


Gráfico 6¿Cuál de los bancos en el sistema hondureño utiliza con mayor regularidad?

- **BAC (40,9%)**: El banco más utilizado por los encuestados es BAC con un 40.9% de participación, este análisis se debe a que es una de las instituciones con una amplia base de clientes, lo que aumenta los casos de fraude.
- **Banco Atlántida (21,7%):** Es una de las instituciones más grandes del mercado; sin embargo, según las encuestas, el 21,7% de los encuestados indican que su uso es menor al del BAC. A pesar de esto, el porcentaje sugiere que también está asociado a una cantidad considerable de casos de fraude.
- **Ficohsa (19,1%):** Tiene una participación del 19,1%, lo que lo coloca en una posición importante. Aunque su porcentaje de uso es menor que el de BAC y Banco Atlántida, sigue siendo relevante debido a que lo utilizan una cantidad considerable de los encuestados.
- **Otros bancos (Bancos de Occidente, Davivienda, Banco del País, Lafise, 18.3%:** Estos bancos forman parte del sistema y representan una porción de los encuestados. Según los resultados de la encuesta, reflejan las preferencias de los usuarios. Se puede señalar que la actividad de fraude en estos bancos podría ser de menor escala y que tambien son vulnerables dependiendo del sistema de seguridad y las medidas implementadas.

Pregunta No. 7 ¿Qué tan seguro(a) se siente de utilizar los servicios de banca en línea?

Tabla No. 7

¿Qué tan seguro(a) se siente de utilizar los servicios de banca en línea?	Cantidad
Muy seguro(a)	15
Algo seguro(a)	50
Neutral	23
Algo inseguro(a)	21
Muy inseguro(a)	6
Total	**115**

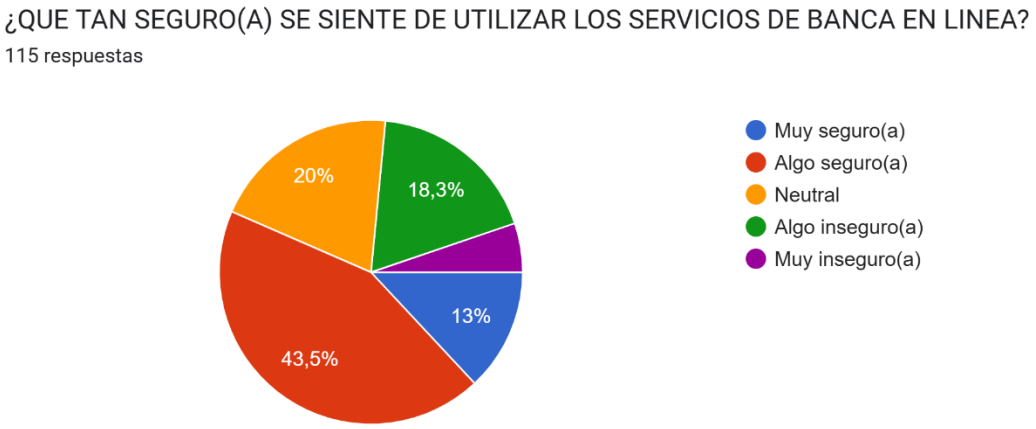


Gráfico 7 ¿Qué tan seguro(a) se siente de utilizar los servicios de banca en línea?

- **43.5%** de los encuestados se sienten algo seguros al utilizar los servicios de banca en línea, siendo esta la categoría con el mayor porcentaje.
- **20%** se siente muy seguro al usarlos, lo que refleja un nivel alto de confianza en las plataformas digitales.
- **18.3%** se sienten neutrales, indicando que estas personas no tienen una opinión clara o definida sobre la seguridad de la banca en línea.
- **13%** se siente algo inseguro, mostrando que existe cierto nivel de preocupación entre los usuarios.
- **5.2%** se siente muy inseguro, un grupo reducido pero importante que percibe altos riesgos en el uso de estos servicios.

Pregunta No. 8 ¿Por qué ha cambiado la contraseña de acceso a la banca en línea?

Tabla No. 8

¿Por qué ha cambiado la contraseña de acceso a la banca en línea?	Cantidad
El banco solicito el cambio por motivos de seguridad	54
Por un intento de hackeo o actividad sospechosa en la cuenta	37
El acceso a la banca en línea se bloqueó tras ingresar incorrectamente la contraseña	24
Total	**115**

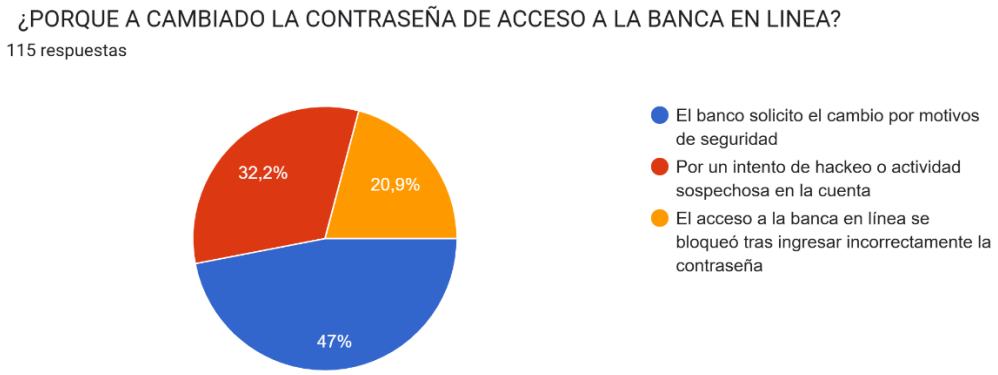


Gráfico 8 ¿Por qué ha cambiado la constraseña de acceso a la banca en línea?

- **El banco solicitó el cambio por motivos de seguridad (54 personas)**: Según los encuestados, por motivos de seguridad la institución bancaria les solicitó cambio de contraseña, esto como parte de prevenir el fraude, alertando a los usuarios de los posibles fraudes.
- **Intento de hackeo o actividad sospechosa en la cuenta (37 personas)**: Un número significativo de los encuestados experimento esta amenaza, y nos indica de implementar medidas de seguridad.
- **El acceso a la banca en línea se bloqueó tras ingresar incorrectamente la contraseña (24 personas)**: Esta situación representa un desafío para los usuarios, ya que el bloqueo se

implementa como una medida para proteger la información de los clientes en la banca en línea.

Pregunta No. 9 ¿Alguna vez ha recibido un correo electrónico, mensaje o llamada sospechosa solicitando información bancaria?

Tabla No. 9

¿**Alguna** vez ha recibido un correo electrónico, mensaje o llamada sospechosa solicitando información bancaria?	Cantidad
Si	172
No	216
Total	**388**

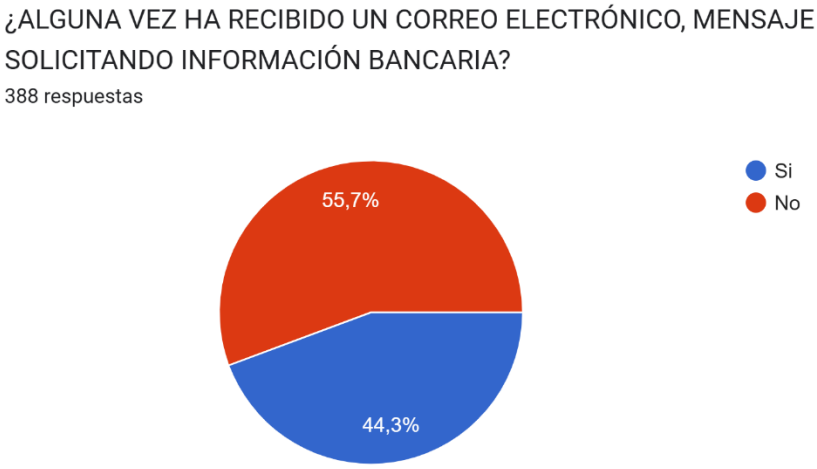


Gráfico 9 ¿Alguna vez ha recibido un correo electrónic, mensaje o llamada sospechosa solicitando información bancaria?

De un total de 388 encuestados, 172 (44%) reportaron haber recibido correos, mensajes o llamadas sospechosas solicitando información bancaria, mientras que 216 (56%) indicaron que no han tenido esta experiencia.

Estos datos revelan que casi la mitad de los encuestados han estado expuestos a intentos de fraude, lo que destaca la necesidad de fortalecer las medidas de seguridad y promover prácticas más robustas de protección de información financiera.

Pregunta No.10 ¿Qué nivel de gravedad considera que tiene el problema del fraude en el sistema Bancario?

Tabla No. 10

¿**Qué** nivel de gravedad considera que tiene el problema del fraude en el sistema bancario?	Cantidad
Muy grave	246
Grave	83
Algo grave	50
Poco grave	7
No es grave	2
Total	**388**

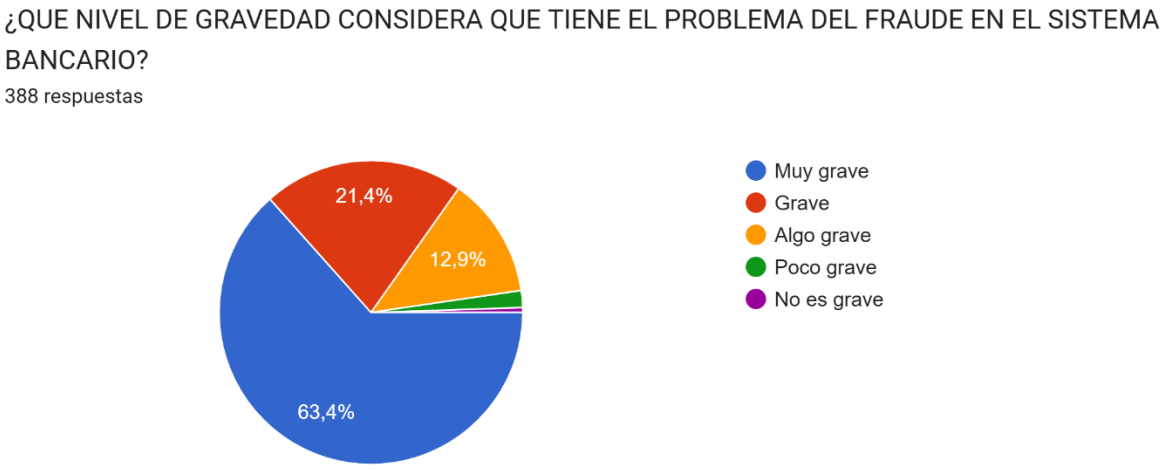


Gráfico 10 ¿Qué nivel de gravedad considera que tiene el problema del fraude en el sistema bancario?

Según los datos de la muestra, se evidencia una marcada preocupación por el fraude en el sistema bancario en Tegucigalpa. De los 388 encuestados, 246 personas (63%) lo calificaron como muy grave, mientras que 83 (21%) lo consideran grave. Por su parte, 50 encuestados (13%) lo perciben como algo grave, y únicamente 7 (2%) lo ven como poco grave. Finalmente, solo 2 personas (0.5%) opinan que "no es grave". Estos resultados reflejan la necesidad de fortalecer las medidas de seguridad y generar confianza en el sistema bancario.

Pregunta No. 11 ¿Considera que su banco le ofrece suficiente información para protegerse contra el fraude?

Tabla No. 11

¿Considera que su banco le ofrece suficiente información para protegerse contra el fraude?	Cantidad
Sí, pero podría ser más	223
Si, suficiente	111
No, no proporcionan información	54
Total	**388**

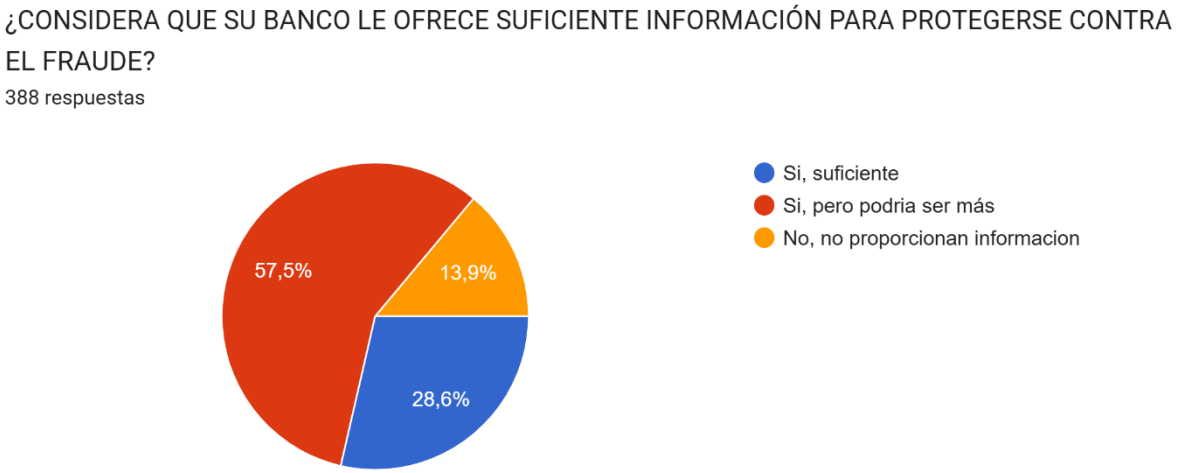


Gráfico 11 ¿Considera que su banco le ofrece suficiente información para protegerse contra el fraude?

De un total de 388 respuestas recibidas, 223 personas (57.5%) consideran que las instituciones bancarias podrían brindar más información sobre cómo los usuarios deben protegerse contra el fraude. Por otro lado, 111 encuestados (28.6%) opinan que las instituciones ya proporcionan suficiente conocimiento para protegerse de las amenazas de la ciberdelincuencia. Finalmente, 54 personas (13.9%) creen que las instituciones bancarias deberían compartir información adicional específicamente sobre la protección de los usuarios en la banca en línea.

Pregunta 12. ¿Qué tan eficaces cree que son las medidas de seguridad que implementa su banco para protegerlo (a) del fraude?

Tabla No. 12

¿Qué tan eficaces cree que son las medidas de seguridad que implementa su banco para protegerlo (a) del fraude?	Cantidad
Muy eficaces	119
Algo eficaces	184
Poco eficaces	53
Nada eficaces	15
No sé	17
Total	**388**

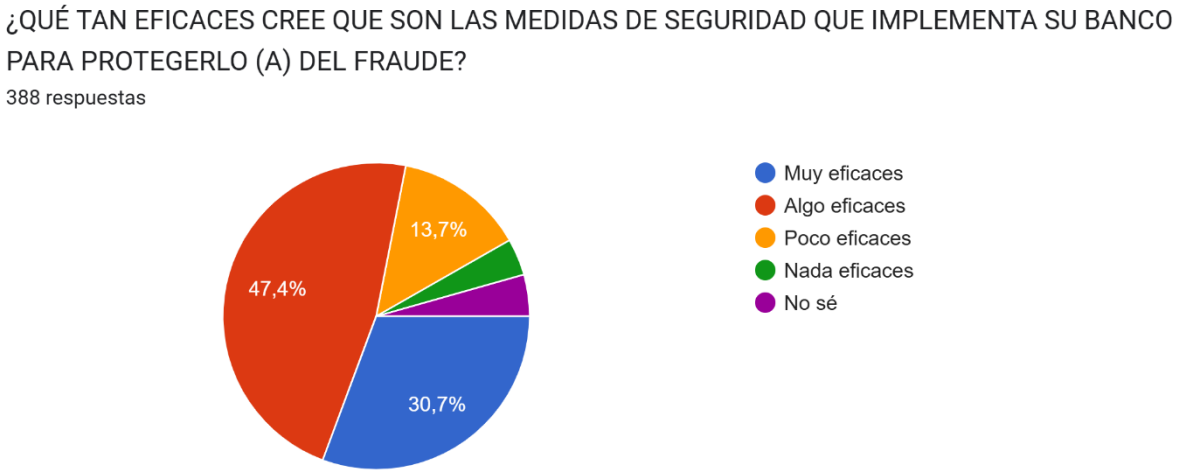


Gráfico 12 ¿Qué tan eficaces cree que son las medidas de seguridad que implementa su banco para protegerlo(a) del fraude?

El 47.4% de la población (184 encuestados) considera que las medidas de seguridad para la protección contra el fraude en la banca en línea implementadas por su banco de preferencia son “algo eficaces”. Por otro lado, el 30.7% (119 encuestados) confía en que las medidas de seguridad son “muy eficaces”. Mientras tanto, el 13.7% (53 encuestados) opina que las medidas de seguridad contra el fraude son “poco eficaces”. La población restante se divide en un 3.9% (15 encuestados) que cree que las medidas de seguridad son “nada eficaces”, y un 4.4% (17 encuestados) que no sabe cómo son las medidas de seguridad.

Pregunta 13. ¿Confía en las notificaciones y alertas de seguridad que recibe de su banco?

Tabla No. 13

¿Confía en las notificaciones y alertas de seguridad que recibe de su banco?	Cantidad
Completamente	100
Moderadamente	209
Algo	62
Nada	17
Total	**388**

Gráfico 13 ¿Confía en las notificaciones y alertas de seguridad que recibe de su banco?

Tras la aplicación de la encuesta, se observó que el 53.9% de los encuestados (209 personas) confía "moderadamente" en las notificaciones y alertas de seguridad que recibe de su banco. Por otro lado, el 25.8% (100 personas) manifiesta una confianza "completa" en estas notificaciones. Sin embargo, el 16% (62 encuestados) señala que confía "algo" en las alertas, reflejando cierto nivel de incertidumbre. Finalmente, el 4.4% de los participantes (17 personas) indica que no confía "nada" en las notificaciones de seguridad enviadas por los bancos.

Pregunta No. 14 ¿Ha recibido charlas o capacitaciones por parte de alguna entidad financiera sobre el fraude bancario?

Tabla No. 14

¿Ha recibido charlas o capacitaciones por parte de alguna entidad financiera sobre el fraude bancario?	Cantidad
Si	283
No	105
Total	**388**

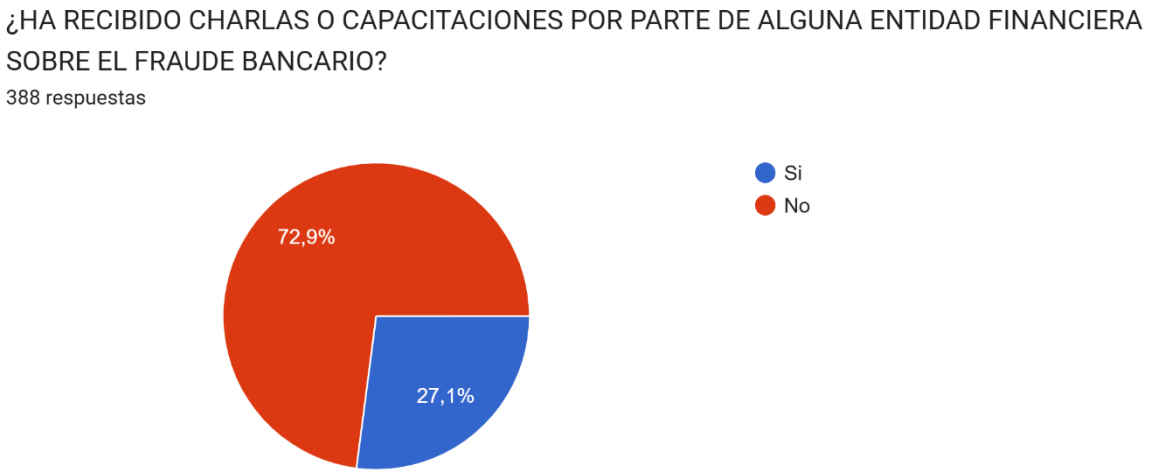


Gráfico 14 ¿Ha recibido charlas o capacitaciones por parte de alguna entidad financiera sobre el fraude bancario?

El gráfico revela que el 72.9% de los encuestados (283 personas) no ha recibido ninguna capacitación sobre el fraude bancario por parte de una entidad financiera. En contraste, el 27.1% (105 personas) sí ha tenido la oportunidad de recibir educación financiera relacionada con este tema por parte de dichas instituciones.

Pregunta No. 15 ¿Qué nivel de conocimiento considera que tiene sobre las prácticas de seguridad para protegerse del fraude bancario?

Tabla No. 15

¿Qué nivel de conocimiento considera que tiene sobre las prácticas de seguridad para protegerse del fraude bancario?	Cantidad
Muy Alto	60
Alto	145
Medio	129
Bajo	42
Muy Bajo	12
Total	**388**

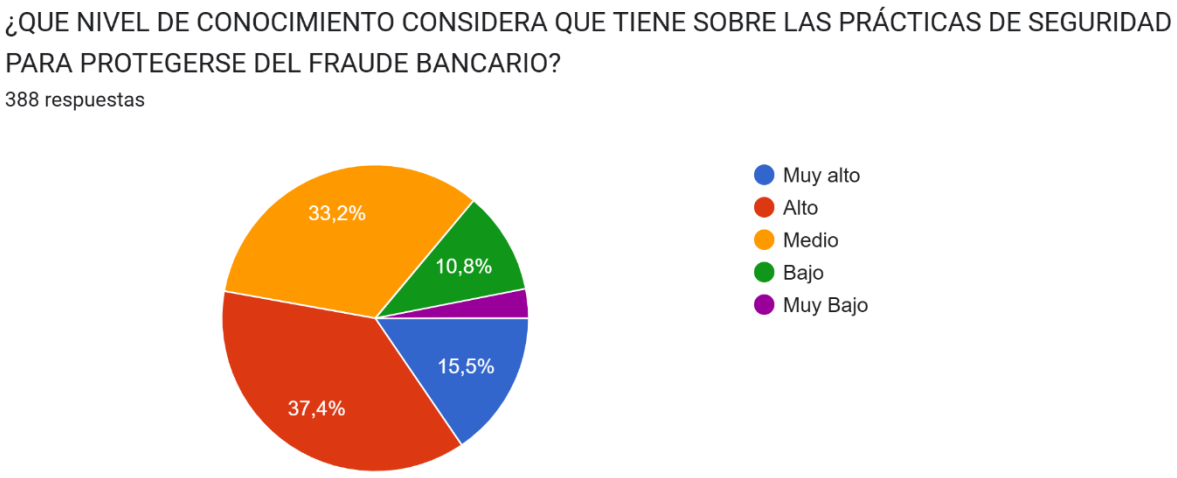


Gráfico 15 ¿Qué nivel de conocimiento considera que tiene sobre las prácticas de seguridad para protegerse del fraude bancario?

Al preguntar a la población sobre su nivel de conocimiento respecto a la seguridad necesaria para protegerse del fraude bancario, los resultados se distribuyeron de la siguiente manera: el 37.4% (145 encuestados) considera que posee un nivel de conocimiento “alto”, mientras que el 33.2% (129 personas) cree tener un nivel “medio”. Por otro lado, el 15.5% (60 encuestados) afirma tener un conocimiento “muy alto” sobre las medidas de protección. Sin embargo, un 10.8% (42 personas) y un 3.1% (12 encuestados) clasifican su conocimiento en las categorías de “bajo” y “muy bajo”, respectivamente.

Pregunta No. 16 ¿Cuáles de las siguientes alternativas considera que son más útiles para evitar el fraude?

Tabla No.16

¿Cuáles de las siguientes alternativas considera que son más útiles para evitar el fraude?	Cantidad
No compartir información confidencial por teléfono o correo electrónico	71
Revisar regularmente los movimientos bancarios.	37
Evitar acceder a la banca en línea desde redes públicas no seguras	34
Todas las anteriores	246
Otros: las herramientas de internet estan muy avanzadas	1
Total	**388**

Gráfico 16 ¿Cuáles de las siguientes alternativas considera que son más utiles para evitar el fraude?

Tras aplicar la encuesta, se observó que la mayoría de la población, un 63.4% (246 encuestados), está de acuerdo en que las mejores prácticas para evitar el fraude incluyen las siguientes acciones: no compartir información por teléfono o correo electrónico, revisar regularmente los movimientos bancarios y evitar acceder a la banca en línea desde redes públicas no seguras.

Por otro lado, el 18% (71 encuestados) considera que la mejor alternativa es no compartir información confidencial por estos medios. El resto de los encuestados se distribuye de la

siguiente manera: el 9.5% (37 personas) cree que es esencial revisar constantemente los movimientos bancarios, y el 8.5% (34 encuestados) opina que se debe evitar acceder a la banca en línea desde redes públicas. Finalmente, un encuestado destacó que las herramientas utilizadas por los ciberdelincuentes son altamente avanzadas.

Pregunta No. 17 ¿Consideraría oportuno que su banco le brinde capacitaciones para prevenir el fraude?

Tabla No. 17

¿Consideraría oportuno que su banco le brinde capacitaciones para prevenir el fraude?	Cantidad
Si	347
No	26
No estoy seguro	15
Total	**388**

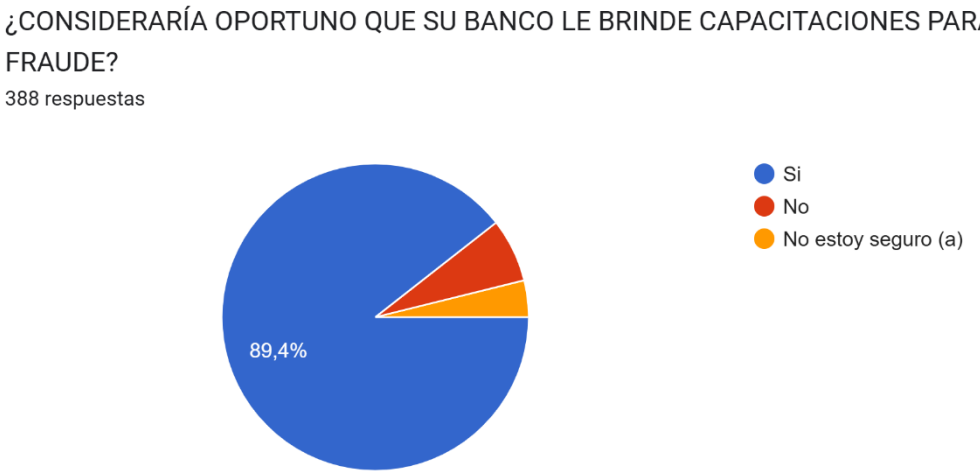


Gráfico 17 ¿Consideraría oportuno que su banco le brinde capacitaciones para prevenir el fraude?

El 89.4% de los encuestados (347 personas) considera que las instituciones bancarias que utilizan regularmente deberían brindar capacitaciones sobre cómo prevenir el fraude bancario. En contraste, el 6.7% (26 personas) opina que no es necesario, mientras que el 3.9% (15 personas) no está seguro de si se deben impartir dichas capacitaciones.

Pregunta No. 18 ¿Cuáles de los siguientes tipos de fraude bancario cree que son más comunes? Seleccione Max 3 opciones

Tabla No. 18

¿Cuáles de las siguientes tipos de fraude bancario cree que son más comunes?	Cantidad
Phishing (fraude por correo electrónico o mensaje de texto)	258
Skimming (clonación de tarjetas en cajeros)	282
Robo de identidad	228
Fraude en transferencias electrónicas	189
Financing Latam (Fraude por Facebook-WhatsApp donde piden que hagan inversiones)	112
Otro: No se	4

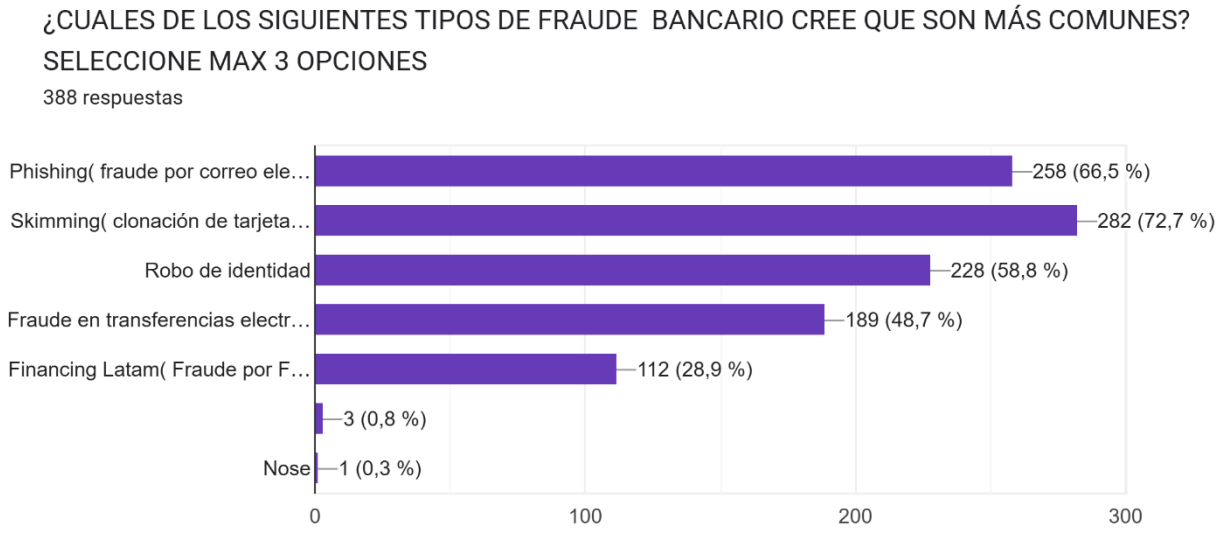


Gráfico 18 ¿Cuáles de los siguientes tipos de fraude bancario cree que son más comunes?

El gráfico presenta los resultados de la encuesta que identifica los tipos de fraude bancario que la población considera más comunes. Con un total de 388 respuestas, el fraude más señalado fue el skimming o clonación de tarjetas, con un 72.7% (282 respuestas). Le sigue el phishing o fraude por correo electrónico, identificado por el 66.5% de los encuestados (258 respuestas). El robo de identidad ocupó el tercer lugar con el 58.8% (228 respuestas), mientras que el fraude en

transferencias electrónicas fue mencionado por el 48.7% (189 respuestas). Un 28.9% (112 respuestas) destacó el fraude relacionado con plataformas como Facebook y WhatsApp, conocido como Financing Latam. Finalmente, solo un 0.8% (3 respuestas) indicó no saber, y un 0.3% (1 respuesta) señaló incertidumbre al respecto.

Pregunta No. 19 ¿Cuál considera que es el principal factor que permite el fraude bancario?

Tabla No. 19

¿Cuál considera que es el principal factor que permite el fraude bancario?	Cantidad
Falta de controles de seguridad en el banco	109
Desconocimiento del cliente	150
Acceso a tecnología avanzada por parte de los defraudadores	128
Otros	1
Total	**388**

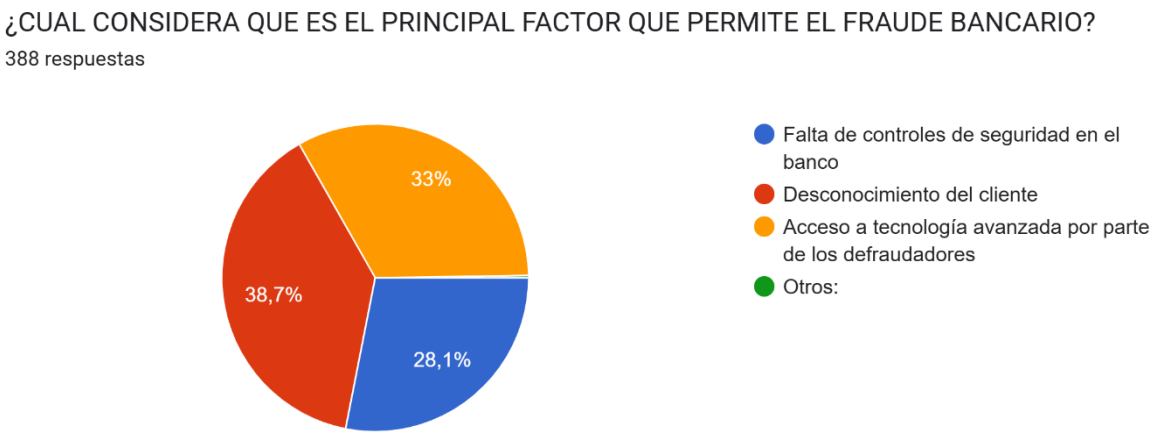


Gráfico 19 ¿Cuál considera que es el principal factor que permite el fraude bancario?

El gráfico refleja los resultados de la encuesta, basada en 388 respuestas, la mayor proporción, un 38.7%, señala el desconocimiento del cliente como el factor que más destaca, evidenciando la importancia de la educación financiera en la prevención del fraude. Le sigue con un 33% el acceso a tecnología avanzada por parte de los defraudadores, lo que resalta la necesidad de que

las instituciones bancarias se mantengan actualizadas frente a las crecientes capacidades tecnológicas de los ciberdelincuentes. En tercer lugar, con un 28.1%, se encuentra la falta de controles de seguridad en el banco, indicando áreas de mejora en los sistemas de protección de las entidades financieras. Finalmente, una pequeña sección del gráfico está representada como otros factores, aunque sin un porcentaje especificado.

Pregunta No. 20 ¿Cuánto confía en que los sistemas de seguridad de su banco evitarán que usted sea víctima de fraude?

Tabla No. 20

¿Cuánto confía en que los sistemas de seguridad de su banco evitarán que usted sea víctima de fraude?	Cantidad
Confío mucho	41
Confío moderadamente	243
Confío poco	79
No confío	25
Total	**388**

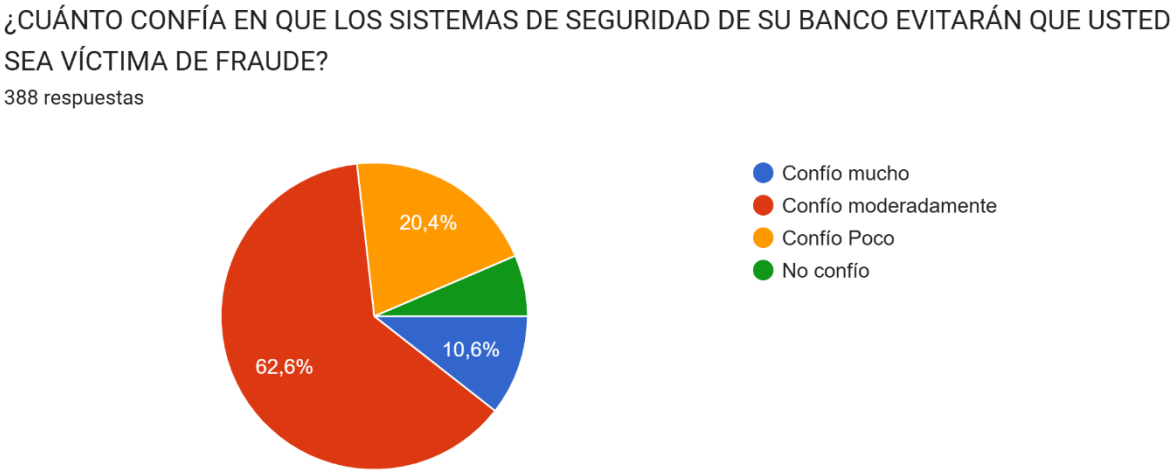


Gráfico 20 ¿Cuánto confía en que los sistemas de seguridad de su banco evitarán que usted sea víctima de fraude?

Con un total de 388 respuestas, los datos revelan que una amplia mayoría, el 62.6% (243 encuestados), confía moderadamente en que los sistemas de seguridad de su banco sean efectivos para protegerlos del fraude. Además, un 20.4% (79 encuestados) indica tener "poca" confianza, mientras que solo un 6.4% (25 encuestados) manifiesta una “no” confianza. Por otro

lado, únicamente el 10.6% (41 encuestados) asegura tener "mucha" confianza en las medidas de seguridad bancaria.

Pregunta No. 21 ¿Qué medidas de prevención considera que deberían implementarse para reducir el fraude en el sistema bancario?

Tabla No. 21

¿Qué medidas de prevención considera que deberían implementarse para reducir el fraude en el sistema bancario?	Cantidad
Aumentar alertas a los usuarios sobre actividades inusuales	101
Capacitación al usuario del sistema bancario	94
Monitoreo tiempo real de las transacciones	86
Establecer canales de denuncia	52
Todas las anteriores	238
Otros	2

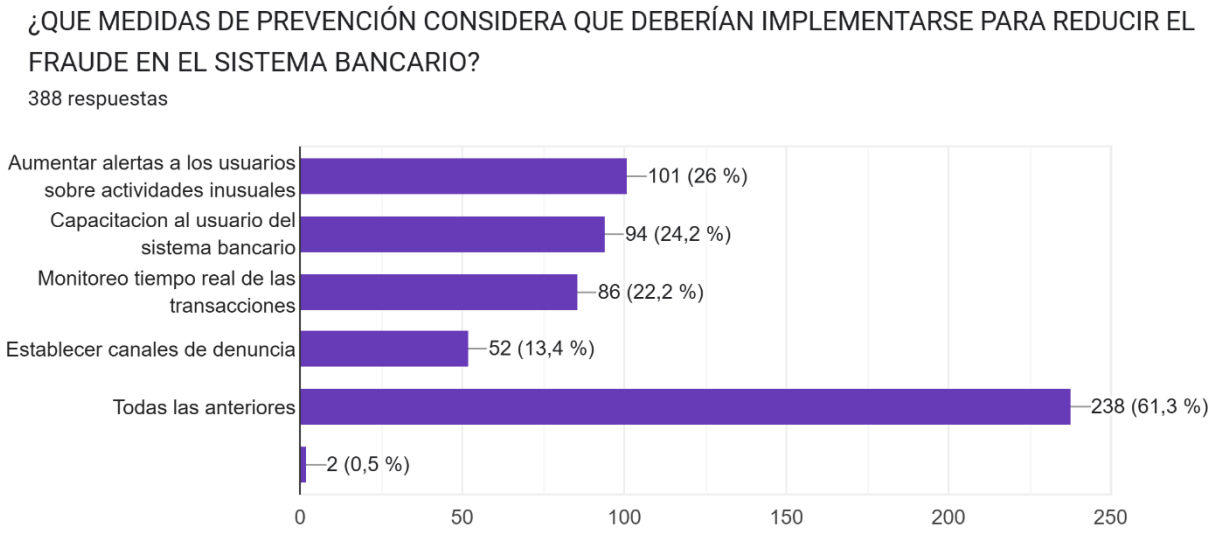


Gráfico 21 ¿Qué medidas de prevención considera que deberían implementarse para reducir el fraude en el sistema bancario?

El gráfico presenta los resultados sobre las medidas de prevención consideradas necesarias para reducir el fraude en el sistema bancario. La opción más seleccionada, con un 61.3% de los

encuestados, fue implementar todas las medidas propuestas, que incluyen aumentar las alertas a los usuarios sobre actividades inusuales, ofrecer capacitación sobre el uso seguro del sistema bancario, monitorear en tiempo real las transacciones y establecer canales de denuncia.

Entre las medidas individuales, la más apoyada fue “aumentar las alertas a los usuarios sobre actividades inusuales”, con un 26% de los votos. A esta le siguió “la capacitación al usuario del sistema bancario”, con un 24.2%, y “el monitoreo en tiempo real de las transacciones”, elegido por el 22.2% de los encuestados. La opción de “establecer canales de denuncia” fue respaldado por un 13.4%, mientras que solo un 0.5% seleccionó la opción de otra medida, sin embargo, no menciono cual sería dicha medida a implementar.

CAPÍTULO VII. CONCLUSIONES

• Métodos de fraude más comunes:

- **Phishing:** Con un aumento del 343.8%, es el principal mecanismo utilizado.
- **Robo de identidad:** Frecuente en transacciones no autorizadas.
- **Fraude interno:** Se estima que el 50% de los casos proviene de empleados bancarios.
- **Skimming y clonación de tarjetas:** Usados para obtener datos y realizar transacciones fraudulentas.

- El fraude en el sistema bancario hondureño representa una amenaza significativa para la confianza de los usuarios y la estabilidad del sector financiero. Las pérdidas económicas afectan tanto a las instituciones financieras como a los clientes, con consecuencias que incluyen pérdida de credibilidad y daño a la reputación. En los años 2023 y 2024, los reclamos por fraudes bancarios aumentaron un 50% en Honduras, siendo el phishing el método más común, representando el 80% de los casos adicionales. Este incremento refleja una creciente vulnerabilidad en los sistemas de seguridad y una falta de educación financiera adecuada entre los usuarios.
- La rápida digitalización de los servicios bancarios ha expuesto las debilidades de los sistemas de seguridad, facilitando la creación de nuevas técnicas fraudulentas como el phishing, el skimming, y las cuentas "mulas", lo que demuestra que los delincuentes están innovando continuamente sus técnicas, lo que requiere una respuesta de seguridad igual de eficiente por parte de las instituciones financieras.
- Los montos de las pérdidas reportadas por los usuarios oscilaron entre L.10,000.00 y L.1,000,000.00. Esto no solo afecta el bienestar financiero de las víctimas, sino también su confianza en el sistema bancario, evidenciando la necesidad de fortalecer las medidas de protección y restaurar la credibilidad en las instituciones financieras.
- A pesar de la implementación de herramientas de autenticación biométrica y detección en tiempo real, los resultados evidencian que estas no son suficientes sin una adecuada educación financiera. Según encuestas, el 67% de los usuarios considera que su nivel de conocimiento sobre prácticas de seguridad es bajo.
- El 58% de los usuarios reportó sentirse inseguro al utilizar servicios de banca en línea, y solo el 42% confía en las medidas de seguridad implementadas por su banco. Esto subraya la urgencia de reforzar la ciberseguridad y mejorar la comunicación con los clientes.

- La falta de conocimiento y concientización de los usuarios sobre prácticas seguras en entornos digitales contribuye significativamente a que sean víctimas de fraude. A pesar de los esfuerzos de los entes regulatorios, persiste un desconocimiento generalizado entre los usuarios sobre los riesgos asociados al uso de canales digitales.
  - La Comisión Nacional de Bancos y Seguros (CNBS) ha establecido lineamientos clave para la mitigación del fraude. Sin embargo, su implementación presenta desafíos, especialmente en la detección temprana y la educación del usuario. Las instituciones bancarias no solo son responsables de implementar medidas de seguridad, sino también de educar a sus clientes sobre los riesgos y cómo protegerse
- Aunque el Código Penal hondureño incluye sanciones para delitos de fraude y suplantación de identidad, se perciben brechas en su aplicación y en la agilidad del sistema judicial para abordar este tipo de crímenes.

CAPÍTULO VIII. RECOMENDACIONES

En el contexto actual, el aumento de los fraudes y amenazas cibernéticas en el sistema bancario exige la implementación de medidas más robustas y efectivas. Estas recomendaciones tienen como objetivo fortalecer la seguridad de las instituciones financieras, proteger a los usuarios y garantizar un entorno bancario más confiable y eficiente. Desde el uso de tecnologías avanzadas como la inteligencia artificial hasta la mejora de los procesos regulatorios y la educación financiera inclusiva, estas acciones buscan abordar los desafíos actuales y futuros de manera integral.

A continuación, se presentan propuestas para fortalecer la ciberseguridad, mejorar las respuestas de fraudes y promover prácticas más seguras y transparentes dentro del sistema financiero.

1. **<u>Fortalecimiento de la ciberseguridad:</u>**

- Actualizar regularmente los sistemas de seguridad de las instituciones bancarias.
- Implementar sistemas de doble autenticación y herramientas avanzadas de detección de transacciones sospechosas.

2. **Adopción de inteligencia artificial (IA):**
- Utilizar tecnologías de IA para analizar patrones de transacciones y detectar actividades sospechosas en tiempo real.
- Incorporar sistemas que aprendan de las tácticas de los delincuentes para prever nuevos tipos de fraude.

3. **Campañas de educación financiera más inclusivas:**
- Incrementar el alcance de las capacitaciones, especialmente en áreas rurales y comunidades con menor acceso a información.
- Promover la creación de materiales educativos interactivos y accesibles sobre la identificación y prevención del fraude bancario.

4. **Atención rápida y eficaz al cliente:**
- Implementar protocolos estandarizados para la denuncia y resolución de casos de fraude en un plazo breve.
- Facilitar herramientas en línea para que los usuarios puedan bloquear sus cuentas inmediatamente ante movimientos sospechosos.

5. **Mejorar los procesos de regulatorios por parte de la CNBS**
- Aumentar la supervisión por parte de la CNBS para asegurar que los bancos cumplan con los lineamientos mínimos de seguridad.
- Aplicar multas a las instituciones que no adopten medidas adecuadas o que sean negligentes ante denuncias de fraude.

6. **Protocolos claros para denuncias:**
- Establecer un sistema único y accesible para que los usuarios puedan denunciar fraudes, con seguimiento transparente y resoluciones en plazos breves.
- Capacitar a empleados bancarios para que puedan ofrecer asistencia inmediata y eficaz a los clientes afectados.

7. **Auditorías de seguridad cibernética obligatorias:**
- Exigir auditorías regulares e independientes de los sistemas de seguridad de las instituciones bancarias.

- Publicar informes sobre el estado de la ciberseguridad en el sistema bancario, aumentando la transparencia.

CAPÍTULO IX. BIBLIOGRÁFIA

(circulares.cnbs.gob.hn), F. (https://www.asjhonduras.com/asj-mitch.html de Noviembre de 2022).

(2023). Obtenido de https://www.bbva.com/es/crecimiento-economico-y-pib-de-que-estamos-hablando/

Aclerk. (28 de octubre de 2024). Obtenido de https://www.detectives-aclerk.com/fraude-y-estafa-entendiendo-las-diferencias/

Amador, M. (29 de marzo de 2023). Obtenido de https://tiempo.hn/reclamos-por-fraude-a-cuentas-bancarias/

Banco Mundial. (4 de Abril de 2023). Obtenido de https://www.bancomundial.org/es/country/honduras/overview

BioCatch. (16 de noviembre de 2024). *BioCatch* . Obtenido de https://www.biocatch.com/digital-banking-fraud-trends-emea-sp

circulares.cnbs.gob.hn). (29 de Mayo de 2023). *https://www.cnbs.gob.hn/educacionfinanciera/evite-riesgos/el-fraude/*. Obtenido de Comision Nacional de Bancos y Seguros.

CNBS. (OCTUBRE de 2006). *(repositorio.cepal.org)*.

CNBS. (24 de marzo de 2023). *Circular CNBS No.003/2023*. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://portalunico.iaip.gob.hn/ver_archivo/MTczMjkyMg==

CNBS. (23 de Marzo de 2023). *CNBS*. Obtenido de https://www.cnbs.gob.hn/comunicado-lineamientos-fraudes-ciberneticos/

CNBS. (25 de Octubre de 2024). Obtenido de https://www.cnbs.gob.hn/educacionfinanciera/evite-riesgos/el-fraude/#:~:text=Es%20cualquier%20acci%C3%B3n%20cometida%20intencionadamente,tercero%20se%20le%20llama%20Fraude.

CNBS. (29 de Octubre de 2024). Obtenido de https://www.cnbs.gob.hn/educacionfinanciera/evite-riesgos/el-fraude/

CNBS. (17 de noviembre de 2024). *CNBS*. Obtenido de https://www.cnbs.gob.hn/educacionfinanciera/

CNBS. (17 de noviembre de 2024). *Reporte de inclusión Financiera 2024*. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnbs.gob.hn/inclusion-financiera/wp-content/uploads/2024/07/REPORTE-DE-INCLUSION-FINANCIERA-2024_FINAL_JULIO-12072024.pdf

Consejo Monetario Centroamericano. (21 de Abril de 2023). Tegucigalpa, Francisco Morazán, Honduras. Obtenido de https://www.secmca.org/imae-de-honduras-47/#:~:text=En%20Honduras%20el%20%C3%8Dndice%20Mensual,4.4%25%20registrado%20doce%20meses%20atr%C3%A1s.

Desarrollo, F. y. (2014). ¿Qué es la economía. En F. y. Desarrollo, *Finanzas y Desarrollo.* Obtenido de https://www.imf.org/external/pubs/ft/fandd/spa/2014/09/pdf/basics.pdf

Economista, E. (23 de 04 de 2019). Obtenido de https://www.worldcomplianceassociation.com/1551/articulo-estafas-millonarias-enron-lehman-brothers-los-diez-fraudes-corporativos-que-sacudieron-al-mundo.html

El pulso. (19 de mayo de 2017). Obtenido de https://www.elpulso.hn/2017/05/19/banhcreser-estafa-corrupcion-e-impunidad-44/

El pulso. (04 de Octubre de 2020). Obtenido de https://www.elpulso.hn/2020/10/04/banco-capital-estafa-corrupcion-e-impunidad-3-4/

El puso. (17 de mayo de 2017). Obtenido de https://www.elpulso.hn/2017/05/17/bancorp-estafa-corrupcion-e-impunidad-24/

Expansión. (s.f.). Obtenido de DatosMacro.com: https://datosmacro.expansion.com/estado/gasto/educacion/honduras#:~:text=En%20referencia%20al%20porcentaje%20que,de%20134%20euros%20por%20habitante.

Expansión. (2023). Obtenido de DatosMacro.com: https://datosmacro.expansion.com/estado/gasto/defensa/honduras

FISCAL, P. D. (Septiembre de 2006). *SECRETARIA DE FINANZAS.* Obtenido de SEFIN: http://www.sefin.gob.hn/wp-content/uploads/Conceptuales/Presupuesto/Clasificador%20Presupuestario.pdf

GANDHI, V. P. (s.f.). *La Ley de Wagner sobre los gastos públicos.* Obtenido de https://www.cepc.gob.es/sites/default/files/2021-12/31709recp058075.pdf

Garrote, A. (10 de octubre de 2024). *La razón*. Obtenido de https://www.larazon.es/economia/que-son-cuentas-mula_202406106666d470e73ed600015babe6.html

Giron, D. (09 de julio de 2024). *Criterio. hn* . Obtenido de https://criterio.hn/delincuentes-ciberneticos-operan-con-impunidad-en-honduras/

GLEIF. (06 de junio de 2024). *Gleif*. Obtenido de https://www.gleif.org/es/newsroom/blog/financial-crime-is-crippling-the-global-economy-breakthrough-identity-tech-is-leading-the-fightback

Heraldo, E. (04 de septiembre de 2024). *El Heraldo*. Obtenido de https://www.elheraldo.hn/sucesos/detenidos-cuatro-exempleados-banco-estafa-lavado-activos-NG21278072

Honduras, C. P. (25 de Octubre de 2024). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/dil/esp/codigo_penal_honduras.pdf

https://www.elpulso.hn/2017/05/16/crisis-bancaria-estafa-corrupcion-e-impunidad-14/. (16 de Mayo de 2017). *El Pulso*.

Idárraga, S. O. (05 de octubre de 2024). *Bllomberg Linea*. Obtenido de https://www.bloomberglinea.com/tecnologia/alertas-diarias-por-fraude-financiero-en-latam-superaron-las-de-norteamerica-en-el-ultimo-ano/

Interpol. (11 de marzo de 2024). *Interpol*. Obtenido de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Evaluacion-de-INTERPOL-sobre-estafas-un-peligro-mundial-incrementado-por-la-tecnologia

Jiménez, F. (2021). Nuevas tendencias: la teoría del crecimiento endógeno. En F. Jiménez, *Elementos de teoría y política macroeconómica para una economía abier.* Perú: Fondo Editorial - Pontificia Universidad Católica del Perú. Obtenido de http://files.pucp.edu.pe/departamento/economia/LDE-2012-02a-19.pdf

La Prensa. (23 de 02 de 2023). Obtenido de https://www.laprensa.hn/honduras/alertan-estafas-bancarias-15-000-190-000-lempiras-honduras-AE12343553

Legislativo, P. (10 de mayo de 2019). *Codigo Penal* . Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

Microblink. (16 de abril de 2024). Obtenido de https://microblink.com/es/resources/blog/los-7-tipos-de-fraude-mas-comunes-en-los-bancos/

Monetario, S. E. (2008). *Informe Económico Regional 2008.* San José, Costa Rica : Secretaría Ejecutiva del Consejo Monetario Centroamericano 3. Obtenido de https://www.secmca.org/wp-content/uploads/2019/02/MacroAnual2008.pdf

Negocios, E. &. (04 de 11 de 2015). *Estrategia & Negocios*. Obtenido de https://www.revistaeyn.com/lasclavesdeldia/honduras-conflicto-en-la-liquidacion-de-banco-continental-FKEN897367

OPS. (2019). Obtenido de https://hia.paho.org/es/paises-2022/perfil-honduras#:~:text=En%20el%202019%2C%20el%20gasto,del%20gasto%20total%20en%20salud.

Penal, C. (28 de Octubre de 2024). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/mmelg/Downloads/C%C3%B3digo%20Penal%20de%201983%20(octubre%202018%20).pdf

Pirani. (15 de noviembre de 2024). Obtenido de https://www.piranirisk.com/es/academia/especiales/los-

4-casos-mas-impactantes-de-fraude-financiero
Publico, M. (31 de marzo de 2023). Obtenido de https://www.mp.hn/publicaciones/entre-10-mil-a-un-millon-de-lempiras-extraen-de-cuentas-bancarias-a-capitalinos/
Quesada, R. B. (Abril de 2006). *El gasto público en Honduras.* Obtenido de https://publications.iadb.org/publications/spanish/viewer/El-gasto-p%C3%BAblico-en-Honduras.pdf
Rodrigo Bolaños Zamora, y. F. (2006). El Gasto Público en Honduras. *Banco Interamericano de Desarollo*, 7.
Rodriguez, L. (26 de julio de 2024). *El Heraldo*. Obtenido de https://www.elheraldo.hn/economia/medidas-recientes-cnbs-combatir-fraude-tarjetas-credito-honduras-OA20574875
RODRÍGUEZ, M. G., & GONZÁLEZ, M. G. (2020). El gasto público social y su incidencia. *Espacios*, 12.
Sarwat Jahan, A. S. (2014). ¿Qué es la economía. En *Finanzas y Desarollo* (págs. 53-54).

CAPÍTULO XII. APLICABILIDAD

En este capítulo se presenta una propuesta para el diseño de un plan de contingencia que permita a las instituciones bancarias fortalecer sus medidas de seguridad frente a situaciones de fraude, buscando proteger a los usuarios, mitigar riesgos financieros y operativos, y garantizar la continuidad de los servicios. Además, dé promover una cultura de prevención dentro de las entidades, de fomentar la transferencia en los departamentos de atención a los usuarios de la banca en línea, lo cual no solo contribuye a la seguridad de las transacciones, sino que también refuerza la credibilidad y la confianza de los clientes en la institución financiera.

12.1 Introducción

El fraude en el sistema bancario se ha convertido en una de las crisis más relevantes de la actualidad, afectando gravemente las finanzas de los usuarios. Este problema no solo genera pérdidas económicas significativas, sino que también debilita la confianza en las instituciones bancarias. Ante el aumento de los casos de fraudes, es crucial que las entidades financieras implementen estrategias efectivas de seguridad y contingencia para proteger a los usuarios y restaurar la credibilidad del sistema bancario.

12.2 Objetivo General

Abordar la creciente crisis del fraude en el sistema bancario, que está afectando gravemente las finanzas de los usuarios y deteriorando la confianza en las instituciones financieras. Este enfoque busca sugerir y fomentar la puesta en marcha de estrategias de seguridad y planes de contingencia eficaces, que permitan a las instituciones bancarias salvaguardar los intereses de los usuarios, reducir los riesgos asociados al fraude y restablecer la credibilidad y la confianza en el sistema bancario

12.3 Objetivo Específicos

- Promover una cultura de prevención y sensibilización dentro de las instituciones bancarias, involucrando a empleados y usuarios en prácticas seguras para la realización de transacciones.

- Establecer indicadores clave de desempeño (KPI) para medir la efectividad del plan de contingencia y las estrategias de seguridad, asegurando un monitoreo constante y ajustes oportunos.

12.4 Propuesta

Tras analizar los resultados de la encuesta, se identificó que un porcentaje de usuarios carece de conocimientos suficientes sobre las medidas preventivas para protegerse del fraude, especialmente en la banca en línea y otros canales digitales. Para reducir los casos de fraude, se propone que las instituciones bancarias: (1) implementen estrategias y procedimientos enfocados en el fortalecimiento de las medidas de seguridad, como la autenticación multifactor y sistemas de monitoreo en tiempo real, y (2) desarrollen una campaña de concientización que eduque a los usuarios sobre prácticas seguras, utilizando herramientas digitales y talleres para aumentar su educación financiera. Estas iniciativas permitirán no solo disminuir los riesgos, sino también mejorar la confianza de los clientes en las plataformas digitales de la banca.

12.5 Plan de acción

Se propone un plan de acción basado en un análisis de riesgos que permita identificar las principales amenazas y evaluar las vulnerabilidades enfrentadas por los usuarios y las instituciones bancarias, tomando como referencia los casos reportados. Este análisis servirá como base para que cada institución desarrolle e implemente estrategias efectivas destinadas a mitigar los riesgos asociados al fraude, protegiendo tanto a los usuarios como a la entidad misma.

Adicionalmente, se plantea el diseño de una campaña integral de educación financiera que tenga un impacto significativo. Esta campaña se llevará a cabo mediante el uso estratégico de redes sociales para alcanzar a un público más amplio y la realización de talleres de simulacro, los cuales proporcionen a los usuarios herramientas prácticas para identificar y prevenir intentos de fraude. Estas acciones buscan no solo disminuir la incidencia de casos de fraude, sino también fortalecer la confianza y la seguridad en las transacciones bancarias

12.6 Descripción del plan de acción

Se debe definir claramente el público meta al que se busca impactar, los medios y métodos que se emplearán para llevar a cabo la campaña de concientización. También debe incluirse una introducción que explique el propósito de la campaña, así como los beneficios esperados al implementarla.

12.6.1 Definición del público meta

La campaña está dirigida a los usuarios que cuentan con banca en línea:
Personas comprendidas entre los 18 y los 75 años de distinto género:

- Usuarios activos de banca en línea
- Potenciales usuarios de banca en línea

12.6.2 Medios para la concientización

Se propone una campaña de concientización que utilice diversos canales para informar y educar a los usuarios de banca en línea. La estrategia incluye:

1. Envío de boletines informativos con temas clave sobre seguridad, buenas prácticas y novedades en los servicios, acompañados de gráficos y enlaces para más información.
2. Publicación en redes sociales de infografías, videos y consejos prácticos, así como videos explicativos cortos sobre cómo detectar fraudes y garantizar transacciones seguras.
3. Incorporación de mensajes breves en las notificaciones de las aplicaciones y portales web, enfatizando prácticas de seguridad, como no compartir contraseñas o reconocer intentos de phishing.
4. Inclusión de banners y pop-ups en las plataformas de banca en línea, mostrando recordatorios al iniciar sesión, como: 'Evite ingresar datos personales en sitios desconocidos.
5. Creación de una sección educativa dentro de las plataformas, donde los usuarios puedan encontrar consejos, tutoriales y preguntas frecuentes sobre seguridad en línea.

.

12.6.3 Modalidad

La campaña puede llevarse a cabo mediante modalidades virtuales, utilizando medios digitales para la difusión y educación de los usuarios. Adicionalmente, se puede aprovechar la realización de ferias de emprendimiento para informar a los asistentes sobre las medidas más recientes de prevención contra el fraude bancario.

Beneficios de la campaña de concientización

- La sociedad aprende a proteger sus datos personales y financieros reduciendo el riesgo de ser futuras víctimas de fraudes o robos. Creando una cultura de prevención en lugar de reaccionar ante incidentes.
- Crear mayor confianza en el sistema bancario mediante el entendimiento de cómo funciona las medidas de seguridad.
- Se obtiene una reducción en errores humanos, los usuarios adoptan mejores prácticas y evitan ingresar datos en sitios inseguros o compartir contraseñas.
- Y se conocen las últimas recomendaciones y herramientas para mantenerse protegidos frente a amenazas emergentes.

12.8 Importancia de la campaña de concientización

1. **La protección de los datos personales**
    - Los usuarios de la banca en línea aprenden a identificar los riesgos como ser: los fraudes, el robo de identidad, etc.
    - Se fomenta a través de las campañas de concientización una cultura preventiva que ayudará a los usuarios en la disminución de los fraudes.
    - Se promueve que el uso de herramientas que ayuden a salvaguardar la información.
2. **Aumenta la confiabilidad en los sistemas**
    - Al adquirir conocimiento el usuario y cómo funciona las medidas de seguridad crece la confianza en las instituciones bancarias.
    - Aumenta la credibilidad en los sistemas, esto debido a la transparencia de los servicios que brinda las instituciones bancarias.

- Se refuerza la relación del cliente, al momento de reportar los incidentes, las instituciones generan un compromiso, lo que genera lealtad de los usuarios.

3. **La prevención de los errores humanos**
   - El usuario de la banca en línea adquiere mejores prácticas al momento de ingresar a los sitios web, el no compartir sus claves de acceso.
   - El no responder correos que soliciten información de sus cuentas bancarias y la desconfianza de enlaces recibidos a través de las redes sociales.
   - La capacitación continua frente a estos ataques, que día a día está afectando a la sociedad hondureña., reduce los errores por descuidos o falta de conocimiento.
4. **La actualización ante las nuevas amenazas**
   - Se promueve el uso de software actualizados, y sistemas de autenticación fiables.
   - Las campañas ayudan a los usuarios a reconocer patrones de nuevas amenazas, como variantes avanzadas de phishing.
   - Los usuarios adquieren habilidades para adaptarse rápidamente a los cambios en el panorama de ciberseguridad minimizando los riesgos.

5. **Impacto de las campañas de concientización digital**
   - Al mantener informados a los usuarios se reducen los ataques cibernéticos.
   - Se cierren brechas de seguridad ya que disminuyen los actos delictivos.
   - Al mismo tiempo se genera comportamientos eticos, responsabilidad en el uso de la tecnología, reduciendo el mal uso de los datos, e información personal de los usuarios de la banca en línea.
   - Se benefician los grupos que tienen menos conocimientos del entorno digital.

Propuesta de la aplicación de la campaña de concientización

1. **Educación y Sensibilización**

- Talleres virtuales: Capacitar a los usuarios de la banca en línea en la identificación de los fraudes más comunes phishing, estafas telefónicas, robo de identidad).
- Charlas a los usuarios que aún no se han adaptado al uso de tecnología.
- Redes sociales: La publicación en las redes sociales, Facebook, etc. Consejos prácticos

alertando a la población de las nuevas formas de fraude.

- Mensajes SMS: Envió de mensajes a los usuarios alertándolos sobre las actividades sospechosas.
- Material educativo: Que cada institución bancaria a través de boletines, informe a los usuarios de cómo prevenir los fraudes.

2. Establecer alianzas estratégicas

- A través de los medios de comunicación: Enviar mensajes cortos a la población hondureña, "**No compartas información de tus cuentas bancarias**"
  Historias dramatizadas: Videos cortos de casos de fraude y el impacto en las víctimas.
- En el sector educativo: A través de la educación financiera, se promueve el conocimiento de los ciberataques.
- Periódicos y revistas locales: Promoviendo el impacto del fraude en el sistema bancario y cómo prevenirlo.
- Programas de radio: Conducidos por expertos en ciberseguridad y finanzas, con el objetivo de alertar a la población hondureña sobre los distintos tipos de fraude y cómo prevenirlos.
- La Comisión Nacional de Bancos y Seguros **(CNBS)**, como ente regulador de las instituciones bancarias, en colaboración con el Gobierno de Honduras, debe liderar iniciativas para fortalecer la educación financiera de la población hondureña.

  Desarrollo de programas educativos enfocados en temas clave como la gestión responsable de recursos financieros, el uso seguro de servicios bancarios y la prevención de fraudes.
  Alianzas estratégicas con instituciones públicas y privadas para ampliar el alcance de las iniciativas, especialmente en comunidades vulnerables o de difícil acceso.

La implementación de un plan de contingencia y campañas de concientización resulta fundamental para combatir el fraude bancario, proteger a los usuarios y fortalecer la confianza en las instituciones financieras. Mediante la adopción de tecnologías avanzadas, como el monitoreo en tiempo real, junto

con programas educativos y campañas de sensibilización, se promueve una cultura de prevención que reduce errores humanos y riesgos operativos.

Además, la colaboración entre las entidades bancarias, entes reguladores y medios de comunicación es esencial para ampliar el alcance de estas iniciativas, especialmente en comunidades vulnerables. Estas acciones ayudan a fortalecer la educación financiera y la seguridad de los servicios el cual ayudará a contribuir a consolidar un sistema bancario más seguro, transparente y confiable.

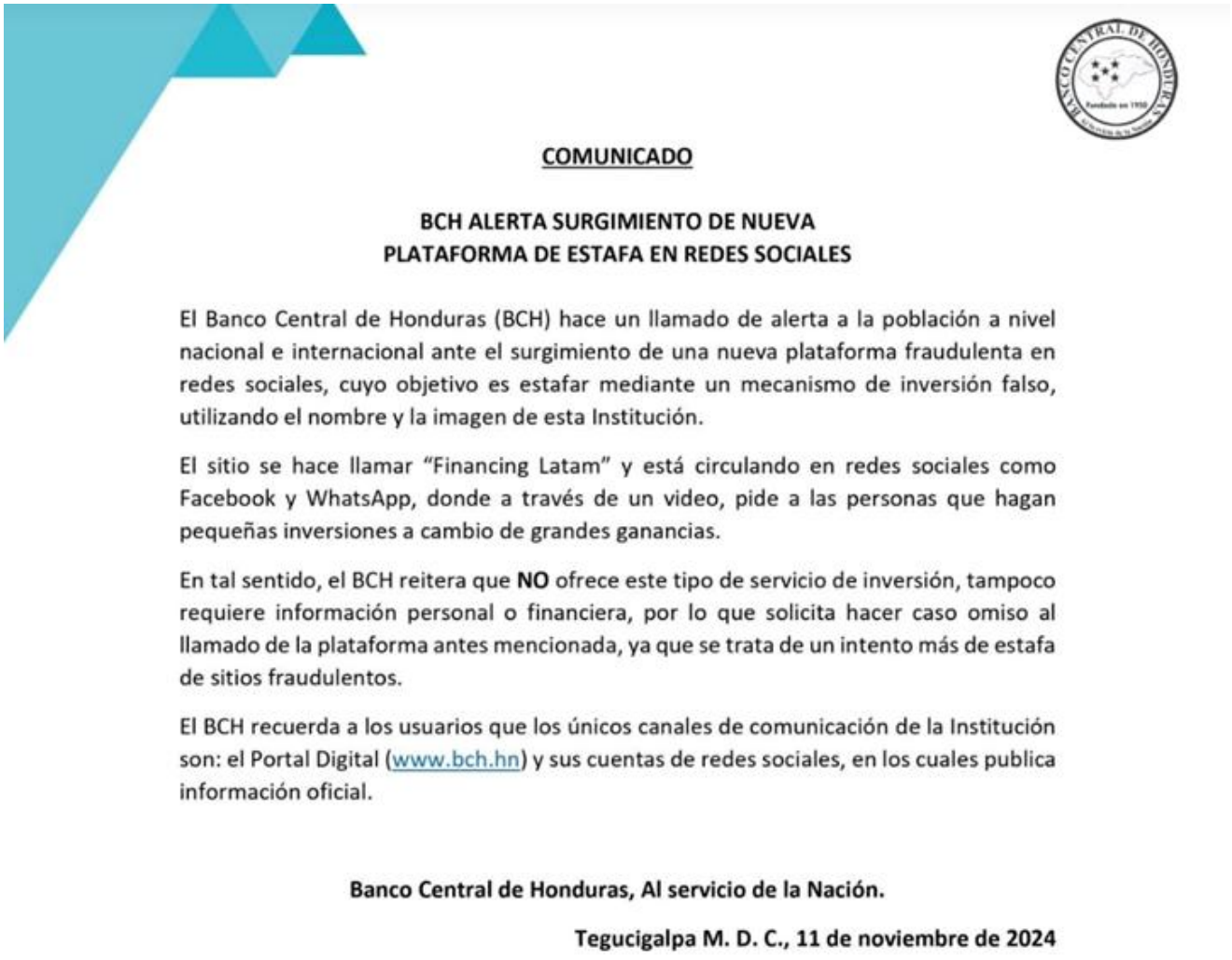
CAPÍTULO XI. ANEXOS

Anexo 1: Tabla de la evolución de los reclamos presentados por los usuarios financieros antes las instituciones supervisadas (En unidades)

Tipo de Reclamo	2020	2021	2022	2023
Depósitos del Público	119	219	293	277
Phishing	61	209	297	1,318
Préstamos	759	766	613	595
Seguros	92	126	132	107
Servicio al Cliente	40	114	242	575
Tarjetas de Crédito/Débito	1,008	981	1,203	1,440
Otros	207	189	219	189
TOTAL	2,286	2,601	2,999	4,501

Fuente: Comisión Nacional de Bancos y Seguros (CNBS)

Anexo 2: Comunicado del BCH 11/11/2024



COMUNICADO

BCH ALERTA SURGIMIENTO DE NUEVA PLATAFORMA DE ESTAFA EN REDES SOCIALES

El Banco Central de Honduras (BCH) hace un llamado de alerta a la población a nivel nacional e internacional ante el surgimiento de una nueva plataforma fraudulenta en redes sociales, cuyo objetivo es estafar mediante un mecanismo de inversión falso, utilizando el nombre y la imagen de esta Institución.

El sitio se hace llamar "Financing Latam" y está circulando en redes sociales como Facebook y WhatsApp, donde a través de un video, pide a las personas que hagan pequeñas inversiones a cambio de grandes ganancias.

En tal sentido, el BCH reitera que **NO** ofrece este tipo de servicio de inversión, tampoco requiere información personal o financiera, por lo que solicita hacer caso omiso al llamado de la plataforma antes mencionada, ya que se trata de un intento más de estafa de sitios fraudulentos.

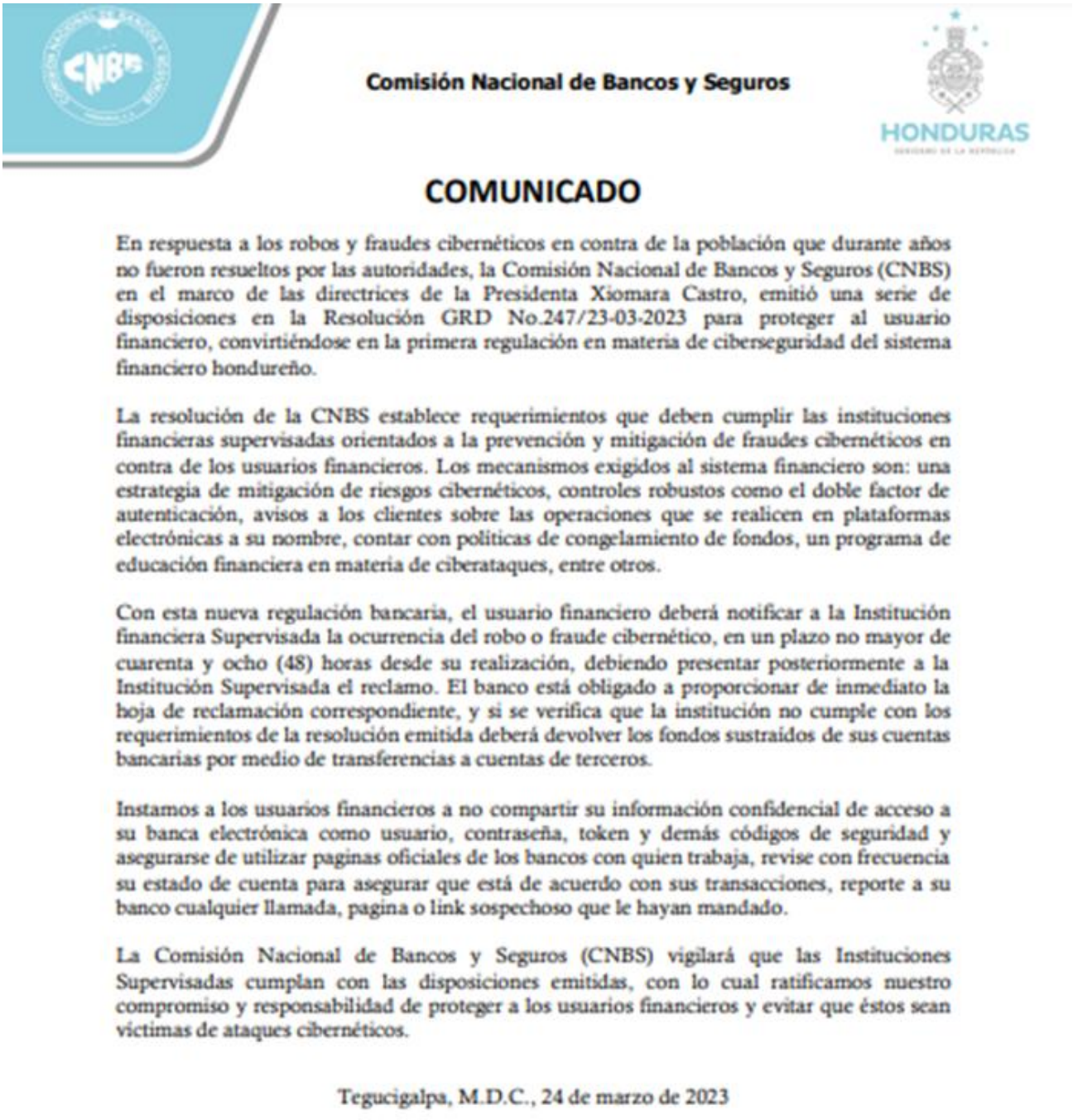
El BCH recuerda a los usuarios que los únicos canales de comunicación de la Institución son: el Portal Digital (www.bch.hn) y sus cuentas de redes sociales, en los cuales publica información oficial.

Banco Central de Honduras, Al servicio de la Nación.

Tegucigalpa M. D. C., 11 de noviembre de 2024

Fuente: Banco Central de Honduras (BCH)

Anexo 3: Comunicado de la CNBS 24/03/2023



Comisión Nacional de Bancos y Seguros

HONDURAS

COMUNICADO

En respuesta a los robos y fraudes cibernéticos en contra de la población que durante años no fueron resueltos por las autoridades, la Comisión Nacional de Bancos y Seguros (CNBS) en el marco de las directrices de la Presidenta Xiomara Castro, emitió una serie de disposiciones en la Resolución GRD No.247/23-03-2023 para proteger al usuario financiero, convirtiéndose en la primera regulación en materia de ciberseguridad del sistema financiero hondureño.

La resolución de la CNBS establece requerimientos que deben cumplir las instituciones financieras supervisadas orientados a la prevención y mitigación de fraudes cibernéticos en contra de los usuarios financieros. Los mecanismos exigidos al sistema financiero son: una estrategia de mitigación de riesgos cibernéticos, controles robustos como el doble factor de autenticación, avisos a los clientes sobre las operaciones que se realicen en plataformas electrónicas a su nombre, contar con políticas de congelamiento de fondos, un programa de educación financiera en materia de ciberataques, entre otros.

Con esta nueva regulación bancaria, el usuario financiero deberá notificar a la Institución financiera Supervisada la ocurrencia del robo o fraude cibernético, en un plazo no mayor de cuarenta y ocho (48) horas desde su realización, debiendo presentar posteriormente a la Institución Supervisada el reclamo. El banco está obligado a proporcionar de inmediato la hoja de reclamación correspondiente, y si se verifica que la institución no cumple con los requerimientos de la resolución emitida deberá devolver los fondos sustraídos de sus cuentas bancarias por medio de transferencias a cuentas de terceros.

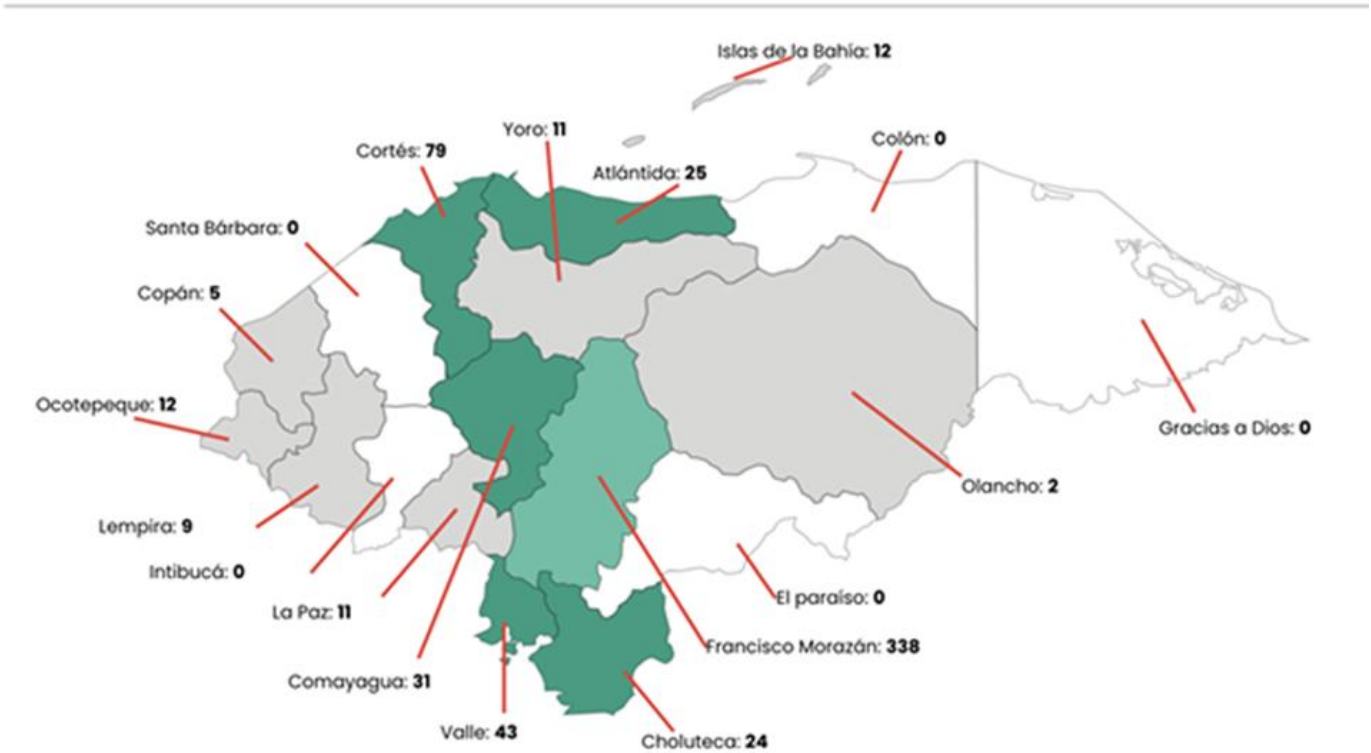
Instamos a los usuarios financieros a no compartir su información confidencial de acceso a su banca electrónica como usuario, contraseña, token y demás códigos de seguridad y asegurarse de utilizar paginas oficiales de los bancos con quien trabaja, revise con frecuencia su estado de cuenta para asegurar que está de acuerdo con sus transacciones, reporte a su banco cualquier llamada, pagina o link sospechoso que le hayan mandado.

La Comisión Nacional de Bancos y Seguros (CNBS) vigilará que las Instituciones Supervisadas cumplan con las disposiciones emitidas, con lo cual ratificamos nuestro compromiso y responsabilidad de proteger a los usuarios financieros y evitar que éstos sean víctimas de ataques cibernéticos.

Tegucigalpa, M.D.C., 24 de marzo de 2023

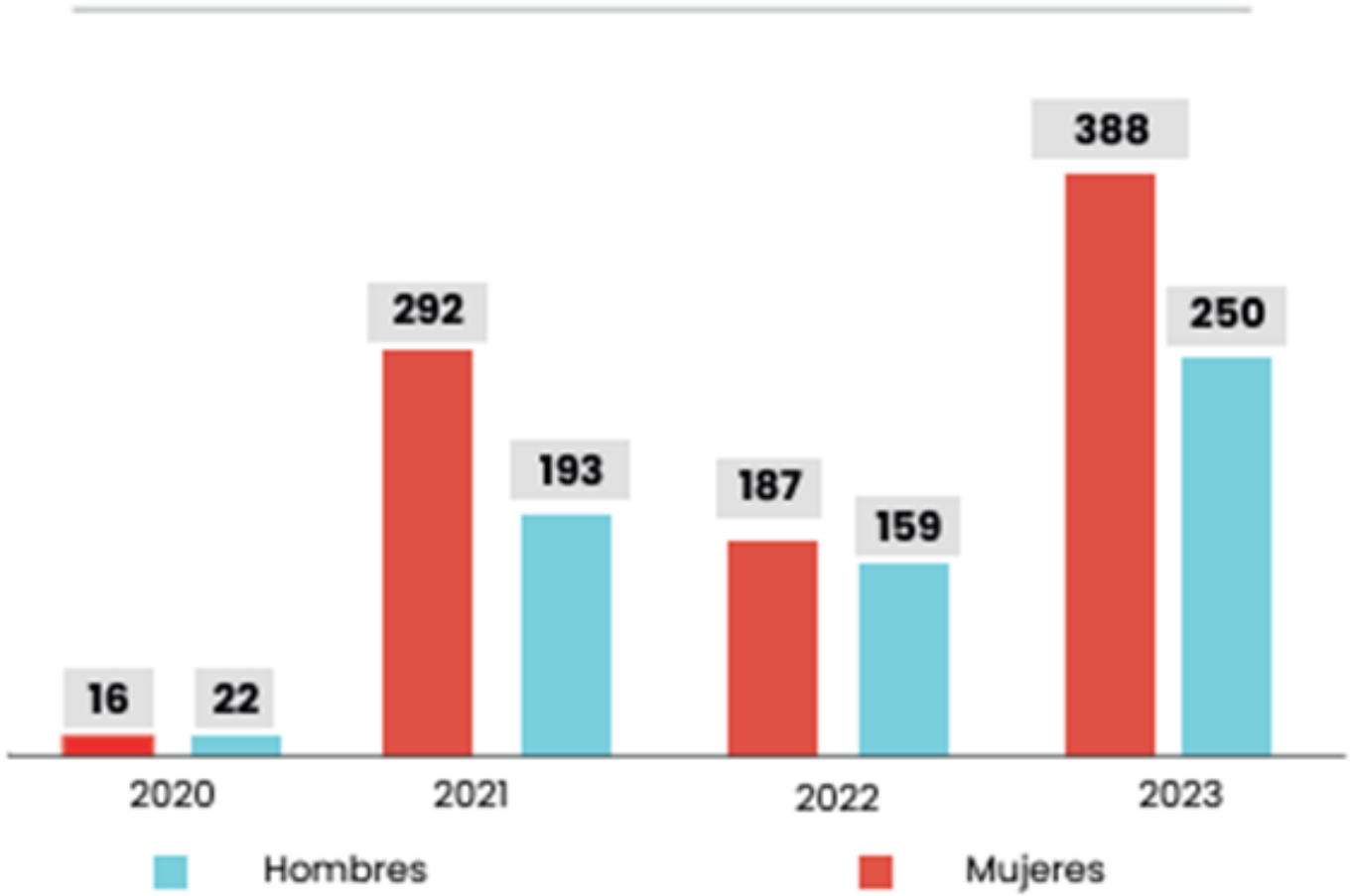
Fuente: Comisión Nacional de Bancos y Seguros (CNBS)

Anexo 4 Número de capacitaciones impartidas en materia de Educación Financiera a nivel departamental 2023.



Fuente: Gerencia de Educación e Inclusión Financiera y Género de la CNBS

Anexo 5 Número de capacitaciones impartidas en el Aula Virtual por sexo durante el periodo de 2020-2023.



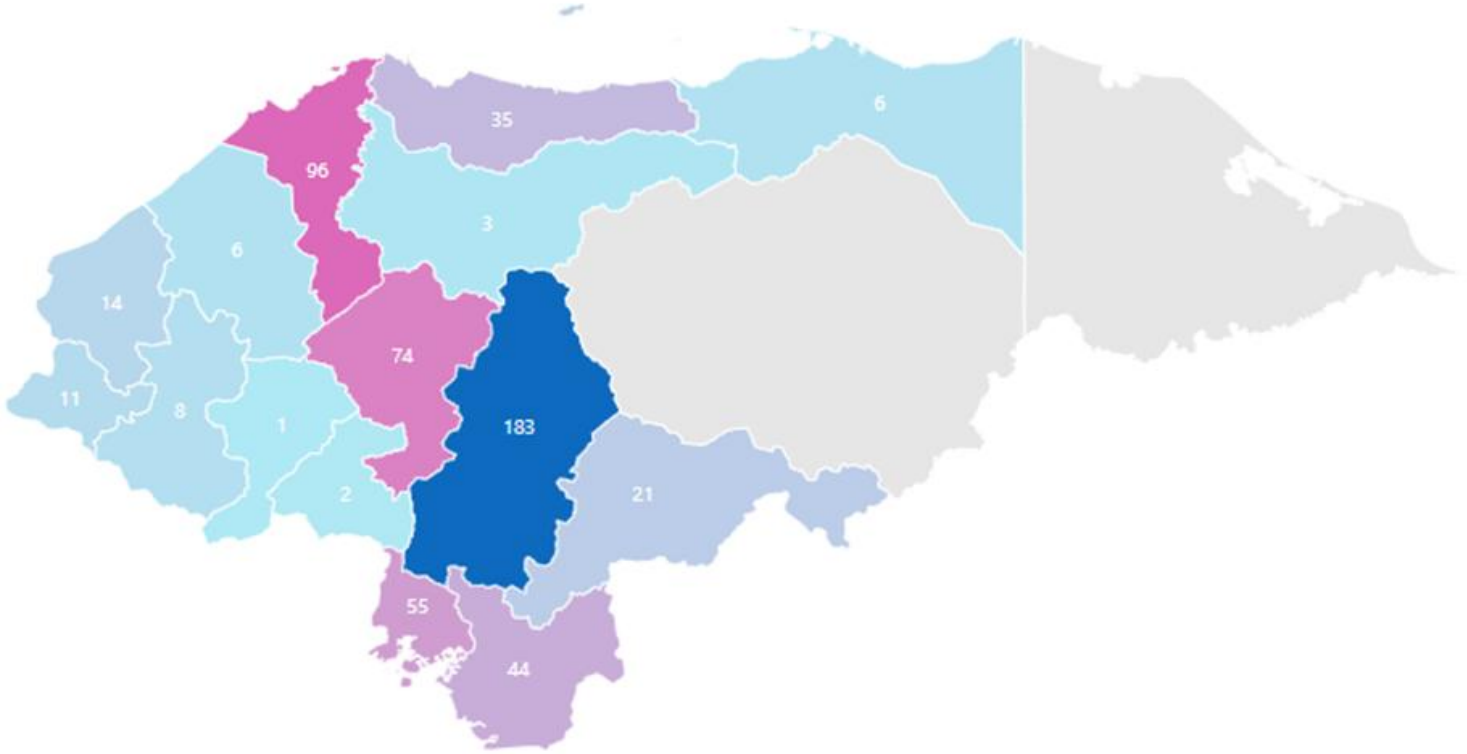
Fuente: Gerencia de Educación e Inclusión Financiera y Género de la CNBS.

Anexo 6 Eventos de Educación Financiera realizada por la CNBS (2021-2023)

	2021	2022	2023
GLOBAL MONEY WEEK	5,390 Participantes	30,750 Participantes	14,470 Participantes
DÍA MUNDIAL DEL AHORRO	17,664 Participantes	36,502 Participantes	66,132 Participantes
Semana de Educación Financiera ¡Tus Finanzas! Nuestro Mayor Interés	No se realizó debido a la pandemia por COVID-19	No se realizó debido a la pandemia por COVID-19	7,953 Participantes

Fuente: Gerencia de Educación e Inclusión Financiera y Género de la CNBS.

Anexo 7 Número de capacitaciones impartidas en materia de Educación Financiera a nivel departamental 2024 hasta noviembre.



Fuente: Gerencia de Educación e Inclusión Financiera y Género de la CNBS.

Anexo 8. Encuesta aplicada a usuarios actuales de la banca en línea

Estudiantes de Contaduría Pública

Estimados participantes, agradecemos su colaboración en esta encuesta, la cual tiene fines académicos y busca evaluar el impacto del fraude en el sistema bancario y su efecto en los usuarios. Su opinión es fundamental para analizar los métodos implementados por el sistema bancario y comprender mejor esta problemática.

1. Sexo
    a) Femenino
    b) Masculino

2. Edad
    a) 18-24 Años
    b) 25-30 Años
    c) 31-36 Años
    d) 37-45 Años
    e) 46-50 Años
    f) 51-60 Años
    g) 60 Años en adelante

3. ¿Usted utiliza banca en línea?

    a) Si
    b) No

4. ¿Alguna vez ha sido víctima de fraude bancario o ha experimentado alguna actividad sospechosa en sus cuentas bancarias?

    a) Si
    b) No

5. ¿Qué acciones tomó la institución bancaria para resolver el caso del fraude? - seleccionar 3 opciones

    a) Detección y Notificación Inmediata
    b) Congelación de la Cuenta Afectada
    c) Investigación Interna
    d) Llenar formulario de reclamación
    e) Reembolso de los fondos
    f) Pasar el caso al ente regulador CNBS

6. ¿Cuál de los bancos en el sistema hondureño utiliza con mayor regularidad?

    a) BAC
    b) Banco Atlántida
    c) Ficohsa
    d) Banco de Occidente
    e) Otro _____

7. ¿Qué tan seguro(a) se siente de utilizar los servicios de banca en línea?

    a) Muy seguro(a)
    b) Algo seguro(a)
    c) Neutral
    d) Algo inseguro(a)
    e) Muy inseguro(a)

8. ¿Por qué ha cambiado la contraseña de acceso a la banca en línea?

    a) El banco solicito el cambio por motivos de seguridad
    b) Por un intento de hackeo o actividad sospechosa en la cuenta
    c) El acceso a la banca en línea se bloqueó tras ingresar incorrectamente la contraseña

9. ¿Alguna vez ha recibido un correo electrónico, mensaje o llamada sospechosa solicitando información bancaria?

    a) Si
    b) No

10. ¿Qué nivel de gravedad considera que tiene el problema del fraude en el sistema bancario?

    a) Muy grave
    b) Grave
    c) Algo grave
    d) Poco grave
    e) No es grave

11. ¿Considera que su banco le ofrece suficiente información para protegerse contra el fraude?

    a) Si, suficiente
    b) Si, pero podría ser más
    c) No, no proporcionan información

12. ¿Qué tan eficaces cree que son las medidas de seguridad que implementa su banco para protegerlo (a) del fraude?

    a) Muy eficaces
    b) Algo eficaces
    c) Poco eficaces
    d) Nada eficaces
    e) No sé

13. ¿Confía en las notificaciones y alertas de seguridad que recibe de su banco?

    a) Completamente
    b) Moderadamente
    c) Algo
    d) Nada

14. ¿Ha recibido charlas o capacitaciones por parte de alguna entidad financiera sobre el fraude bancario?

    a) Si
    b) No

15. ¿Qué nivel de conocimiento considera que tiene sobre las prácticas de seguridad para protegerse del fraude bancario?

    a) Muy alto
    b) Alto
    c) Medio
    d) Bajo
    e) Muy Bajo

16. ¿Cuáles de las siguientes alternativas considera que son más útiles para evitar el fraude?

    a) No compartir información confidencial por teléfono o correo electrónico
    b) Revisar regularmente los movimientos bancarios.
    c) Evitar acceder a la banca en línea desde redes públicas no seguras
    d) Todas las anteriores
    e) Otros

17. ¿Consideraría oportuno que su banco le brinde capacitaciones para prevenir el fraude?

    a) Si
    b) No
    c) No estoy seguro

18. ¿Cuáles de los siguientes tipos de fraude bancario cree que son más comunes? Seleccione máx 3 opciones

    a) Phishing (fraude por correo electrónico o mensaje de texto)
    b) Skimming (clonación de tarjetas en cajeros)
    c) Robo de identidad
    d) Fraude en transferencias electrónicas
    e) Financing Latam (Fraude por Facebook-WhatsApp donde piden que hagan inversiones)
    f) Otro

19. ¿Cuál considera que es el principal factor que permite el fraude bancario?

    a) Falta de controles de seguridad en el banco
    b) Desconocimiento del cliente
    c) Acceso a tecnología avanzada por parte de los defraudadores
    d) Otros

20. ¿Cuánto confía en que los sistemas de seguridad de su banco evitarán que usted sea víctima de fraude?

    a) Confío mucho
    b) Confío moderadamente
    c) Confío Poco
    d) No confío

21. ¿Qué medidas de prevención considera que deberían implementarse para reducir el fraude en el sistema bancario?

    a) Aumentar alertas a los usuarios sobre actividades inusuales
    b) Capacitación al usuario del sistema bancario
    c) Monitoreo tiempo real de las transacciones
    d) Establecer canales de denuncia
    e) Todas las anteriores
    f) Otros