UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024

TESIS PRESENTADA POR:

Bach. KATIA FIORELA APAZA FLORES

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADA

JULIACA – PERÚ

2025

UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024

TESIS PRESENTADA POR:

Bach. KATIA FIORELA APAZA FLORES

PARA OPTAR EL TÍTULO PROFESIONAL DE

ABOGADA

APROBADA POR EL JURADO REVISOR:

PRESIDENTE DEL JURADO : _____
Dr. JOSE DOMINGO CHOQUEHUANCA CALCINA

PRIMER MIEMBRO : _____
Dr. WALTHER MARCELINO NIETO PORTOCARRERO

SEGUNDO MIEMBRO : _____
Dr. HUGO NEPTALI CAVERO AYBAR

ASESOR DE TESIS : _____
Dr. FÉLIX CRISTOBAL OCHATOMA PARAVICINO

LÍNEA DE INVESTIGACIÓN : DERECHO PÚBLICO - P05

RESOLUCIÓN Nº 00149-2025-D/FCJP-UANCV

Juliaca, 22 de agosto de 2025.

Vistos: El expediente. **2025-c-2325** presentado por la Bachiller en Derecho **Srta. KATIA FIORELA APAZA FLORES,** quien solicita nominación de jurados. fecha y hora para rendir el examen de sustentación de borrador de tesis denominado: **VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024**, línea de investigación: **DERECHO PÚBLICO - P05**, para optar el Título Profesional de **ABOGADA** y;

CONSIDERANDO:

Que, de conformidad al Reglamento de Grados y Títulos de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, concordante con el Reglamento General de Grados y Títulos de la UANCV, es procedente acceder a la petición del interesado.

Y estando, la opinión favorable del Director de la Unidad de Investigación y el Decano de la Facultad de Ciencias Jurídicas y Políticas y las atribuciones que confiere el artículo 28º del Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos, Resolución Nº 0294-2023-UANCV-CU-R.

RESUELVE:

Primero.- **DECLARAR APTO** el informe final de la investigación (Borrador de Tesis), por tanto debe señalarse lugar, día y hora para la sustentación del borrador de tesis, en forma presencial, presentado por la Bach. **Srta. KATIA FIORELA APAZA FLORES,** para optar el Título Profesional de **ABOGADA**, el mismo que se llevará a cabo el próximo **miércoles, 27 de Agosto de 2025 a las 4:30:00 PM.** lugar **FILIAL PUNO - SALON DE GRADOS JR. TACNA Nº 787.**

Segundo.- Designar como Jurados, para la evaluación del examen de sustentación de tesis referido, Integrado por los siguientes docentes:

Presidente del jurado : **Dr. JOSE DOMINGO CHOQUEHUANCA CALCINA**

Primer miembro : **Dr. WALTHER MARCELINO NIETO PORTOCARRERO**

Segundo miembro : **Dr. HUGO NEPTALI CAVERO AYBAR**

ASESOR:

Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO

Tercero.- La Comisión de Grados y Títulos de la Facultad, Secretaria Académica y Administrativa quedan encargadas del cumplimiento de la presente resolución.

Regístrese, comuniquese y archivese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
DECANO
FAC. CIENCIAS JURÍDICAS Y POLÍTICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

UNIVERSIDAD ANDINA "Néstor Cáceres Velásquez"
Facultad de Ciencias Jurídicas y Políticas
UNIDAD DE INVESTIGACIÓN

DERECHO

RESOLUCIÓN Nº 0165-2025-UI-FCJP-UANCV-J

Juliaca, 24 de abril de 2025

VISTOS:

El Expediente: **2025-CU-1272** de fecha **27 de marzo de 2025**, presentado por la **Bach. KATIA FIORELA APAZA FLORES,** quien solicita Revisión del Informe Final de la Investigación (borrador de Tesis) y el **Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)"** que fue revisada por el Comité de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, la **Bach.** KATIA FIORELA APAZA FLORES, quien solicita la revisión del Informe Final de la Investigación (borrador de Tesis) del tema titulado**: VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024**, línea de investigación: **- P05,** conducente para optar el Título profesional de **ABOGADA.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable al Informe Final de la Investigación (borrador de Tesis).

Que, el Director de la Unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, corroboro el asesoramiento en el Informe Final de la Investigación (borrador de Tesis) del ASESOR Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO,

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR EL INFORME FINAL DE LA INVESTIGACIÓN (BORRADOR DE TESIS) para la **REVISIÓN DE SIMILITUD TURNITIN**, del tema titulado: **VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024**, presentado por la **Bach. KATIA FIORELA APAZA FLORES**, para optar el Título Profesional de **ABOGADA**, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RATIFICAR, como ASESOR al **Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO.**

ARTICULO TERCERO.- DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
Dr. José Domingo Choquehuanca Calcina
DECANO
FAC. Cs JURÍDICAS Y POLÍTICAS

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
FAC. Cs JURÍDICAS Y POLÍTICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

UNIVERSIDAD ANDINA "Néstor Cáceres Velásquez"
Facultad de Ciencias Jurídicas y Políticas
UNIDAD DE INVESTIGACIÓN

DERECHO

RESOLUCIÓN Nº 787-2024-UI-FCJP-UANCV-J

Juliaca, 29 de noviembre de 2024

VISTOS:

El Expediente: **2024-CU-16356** de fecha **11 de noviembre de 2024**, el cual solicita Revisión de propuesta de Investigación y el **Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación"** que fue revisada por el Comité de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, la **Bach.** KATIA FIORELA APAZA FLORES, quien solicita la revisión y aprobación de la propuesta de Investigación de **Título: VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024**, conducente para optar el Título profesional de **ABOGADA.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable a la propuesta de investigación.

Que, el Director de la Unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, corroboro la propuesta del ASESOR Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO, quien debe estar acreditado y facultado para orientar y ayudar al asesorado en el proceso de elaboración del trabajo de investigación (Tesis) de acuerdo a la DIRECTIVA Nº 004-2019-UANCV-VRAD-OI; y,

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR LA EJECUCIÓN DE LA PROPUESTA DE INVESTIGACIÓN, titulado: **VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024**, presentado por la **Bach. KATIA FIORELA APAZA FLORES**, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RECONOCER, como ASESOR al **Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO**.

ARTICULO TERCERO.- DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
DECANO
Dr. JAVIER ROMULO QUISPE ZAPANA
DECANO
FAC Cs JURIDICAS Y POLITICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

19% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

12% Fuentes de Internet
4% Publicaciones
15% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos complementarios - UANCV

TITULO	
VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024	
Datos de autor	
Nombres y Apellidos	KATIA FIORELA APAZA FLORES
Tipo de documento de identidad	DNI
Número de documento de identidad	44609102
URL de ORCID	https://orcid.org/0009-0000-5409-248X
Datos de asesor	
Nombres y apellidos	FELIX CRISTOBAL OCHATOMA PARAVICINO
Tipo de documento de identidad	DNI
Número de documento de identidad	02436114
URL de ORCID	https://orcid.org/0000-0003-0655-8198
Datos del jurado	
Presidente del jurado	
Nombres Y Apellidos	JOSE DOMINGO CHOQUEHUANCA CALCINA
Tipo de documento	DNI
Número de documento de identidad	02430962
Miembro del jurado 1	
Nombres Y Apellidos	WALTHER MARCELINO NIETO PORTOCARRERO
Tipo de documento	DNI
Número de documento de identidad	23945399
Miembro del jurado 2	
Nombres Y Apellidos	HUGO NEPTALI CAVERO AYBAR
Tipo de documento	DNI
Número de documento de identidad	01332589

Datos de investigación	
Línea de investigación	DERECHO PÚBLICO - P05
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	**Dirección**: PUNO **País**: Perú **Departamento:** Puno **Provincia**: Puno **Distrito**: Puno **Coordenadas.** **Latitud:** -15.84060 **Longitud:** -70.02237 https://maps.app.goo.gl/NX15mNc8C1LM8ppf6 
Año o rango de años en que se realizó la investigación	Noviembre 2024 – Agosto 2025
URL de disciplinas OCDE https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html - Librería	Derecho https://purl.org/pe-repo/ocde/ford#5.05.00 Derecho https://purl.org/pe-repo/ocde/ford#5.05.01

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
Mg. LUIS CHAYNA AGUILAR
DIRECTOR (o)
UNIDAD DE INVESTIGACIÓN
FAC. Cs. JURÍDICAS Y POLÍTICAS

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo KATIA FIORELA APAZA FLORES, identificado con DNI Nro. 44609102 en mi condición de egresado de:

☒ **Escuela Profesional**

☐ **Programa de Segunda Especialidad**

☐ **Programa de Maestría o Doctorado**

DERECHO,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación,** ☐ **Trabajo Académico** denominada:

VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024

Asesorado por: Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca 15 de SETIEMBRE del 2025

Firma del Asesor (Obligatoria)

Firma (Obligatoria)

Huella

DEDICATORIA

Dedico este trabajo a todos aquellos que, de una forma u otra, luchan por la dignidad y los derechos de los trabajadores vulnerables.

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a todos mis seres queridos que hicieron posible la realización de esta tesis.

ÍNDICE GENERAL

CAPÍTULO III

METODOLOGÍA

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ABREVIATURAS

BBVA Banco Bilbao Vizcaya Argentaria

MINJUS Ministerio de Justicia y Derechos Humanos

OEA Organización de Estados Americanos

RAE Real Academia Española

UNODC Oficina de las Naciones Unidas contra la Droga y el Delito

RESUMEN

Objetivo general: establecer la relación entre la impunidad de la ciberdelincuencia financiera y la vulneración a la seguridad bancaria, Puno 2024. **Material y métodos**: se utilizó un cuestionario dirigido a 29 clientes bancarios que utilizan el servicio del Banco de Crédito del Perú de Puno. Este proceso se basó en la adopción de un enfoque cuantitativo y en la aplicación del método hipotético-deductivo. **Resultados**: en un 56.9% indican que la mayoría de los clientes del BCP en Puno están al tanto de los delitos cibernéticos financieros y han experimentado o conocido casos de ciberataques. El 56.9% muestran que una mayoría de los clientes perciben que los ataques cibernéticos afectan la seguridad de las cuentas bancarias y tienen un impacto financiero significativo. El 61.45% muestran una baja confianza y conocimiento entre los clientes del BCP en Puno respecto a la seguridad de las transacciones en línea y las medidas de protección del banco frente a la ciberdelincuencia. Y el 62.08% reflejan una baja satisfacción entre los clientes con respecto a la respuesta del BCP ante ataques cibernéticos. **Conclusiones**: se estableció que la ciberdelincuencia financiera se relaciona significativamente con la vulneración a la seguridad bancaria, Puno 2024. Esto se debe a que se obtuvo un resultado de 0.678 en la prueba de Rho, con un valor p de 0.000 ($p<0.05$); esto implica que cuando aumentan los casos de ciberdelincuencia financiera aumenten, se reduce la seguridad bancaria (correlación inversa).

Palabras clave: ciberdelincuencia, banco, impunidad, seguridad bancaria.

ABSTRACT

General objective: establish the relationship between the impunity of financial cybercrime and the violation of banking security, Puno 2024. **Material and methods:** a questionnaire was used aimed at 29 banking clients who use the service of the Banco de Crédito del Perú in Puno. This process was based on the adoption of a quantitative approach and the application of the hypothetico-deductive method. **Results:** 56.9% indicate that the majority of BCP clients in Puno are aware of financial cybercrimes and have experienced or known cases of cyberattacks. 56.9% show that a majority of customers perceive that cyber-attacks affect the security of bank accounts and have a significant financial impact. 61.45% show low confidence and knowledge among BCP clients in Puno regarding the security of online transactions and the bank's protection measures against cybercrime. And 62.08% reflect low satisfaction among clients regarding BCP's response to cyber-attacks. **Conclusions:** it was established that financial cybercrime is significantly related to the violation of banking security, Puno 2024. This is because a result of 0.678 was obtained in the Rho test, with a p value of 0.000 ($p<0.05$); This implies that when cases of financial cybercrime increase, banking security is reduced (inverse correlation).

Keywords: cybercrime, bank, impunity, banking security.

INTRODUCCIÓN

La digitalización progresiva de los servicios financieros ha revolucionado el sector bancario a nivel global, brindando a los usuarios mayor facilidad y acceso a sus cuentas y transacciones. No obstante, este progreso ha traído consigo nuevos desafíos y riesgos vinculados a la ciberdelincuencia financiera, un problema en constante crecimiento que pone en peligro tanto la seguridad de las plataformas bancarias como la protección de los datos personales y financieros de los clientes.

Esta investigación, se enfocó en la vulnerabilidad de la seguridad bancaria en Puno frente a la ciberdelincuencia financiera; además se analizó el impacto de las amenazas cibernéticas tanto en la protección de las instituciones como en la confianza de los clientes. Asimismo, mediante un análisis exhaustivo de los incidentes de ciberdelincuencia y sus efectos, se pretende, en consecuencia, profundizar en la comprensión de la naturaleza de estos ataques y evaluar, por lo tanto, la efectividad de las medidas de seguridad adoptadas.

La Universidad Andina Néstor Cáceres Velásquez diseñó el modelo que sigue este estudio, que se divide en cuatro secciones fundamentales, cada una de las cuales tiene por objeto ofrecer una comprensión exhaustiva del tema tratado. A continuación se ofrece una breve descripción general de cada una de estas secciones:

Aspectos Generales:

La sección inicial establece el marco de referencia de la investigación, justificando su importancia y definiendo claramente los objetivos que se

persiguen. Se proporciona una visión global del estudio, enfatizando la relevancia del tema y los propósitos del análisis.

Fundamentos Teóricos:

En esta segunda sección, se realiza un análisis profundo de los conceptos clave relacionados con vulneración de la seguridad bancaria e impunidad de la ciberdelincuencia financiera. Se exploran teorías pertinentes, normativas legales aplicables y la literatura académica existente, lo que permite construir una base teórica robusta para la investigación.

Metodología de Investigación:

En esta parte se describe con precisión la estrategia metodológica utilizada en la investigación. Se explican los métodos empleados para recopilar datos, el proceso de selección de fuentes y las metodologías utilizadas para el análisis. Esta explicación sirve para aclarar el enfoque metodológico y cómo se respondieron los problemas que se plantearon.

Análisis de Resultados y Discusión:

La última parte del informe presenta y evalúa los resultados obtenidos a lo largo del proceso de estudio. Se utilizan gráficos y tablas para facilitar la comprensión de los datos recopilados en relación con las preguntas de investigación. A continuación, se examinan los datos. Además, se lleva a cabo un análisis exhaustivo de los resultados, haciendo hincapié en las implicaciones e interpretaciones de los hallazgos, y se presentan las conclusiones y sugerencias basadas en el análisis.

CAPÍTULO I

ASPECTOS GENERALES

1.1. Descripción del problema

En la actualidad, el avance de la digitalización y la creciente dependencia de tecnologías emergentes han facilitado el surgimiento de mayores oportunidades para que los ciberdelincuentes realicen actividades fraudulentas y ataques cada vez más complejos (OEA, 2014). Este hecho no solo pone en riesgo a las instituciones financieras desde el punto de vista de la seguridad, sino que también reduce la confianza que ustedes tienen en los sistemas bancarios. La seguridad de las transacciones financieras y la información personal se ven comprometidas como resultado del crecimiento persistente de los ataques, que se prevé que continúen en los próximos años. Según un estudio publicado por (ESENTIRE 2024), se prevé que el coste mundial de la ciberdelincuencia alcance los 10,5 billones de dólares en 2025. En particular, los ataques dirigidos a instituciones financieras han experimentado un incremento del 72% en los últimos tres años, junto con una notable sofisticación en las técnicas empleadas por los ciberdelincuentes (OEA, 2018). Esta situación genera una preocupación cada vez mayor entre bancos y clientes, quienes se ven expuestos a riesgos constantes de violaciones de seguridad.

Por otro lado, Arnal (2024) señala que los ataques dirigidos a instituciones financieras constituyen el 20% de todos los incidentes registrados en el ámbito de la ciberseguridad. Los datos revelan que las amenazas más frecuentes incluyen phishing, malware y ransomware, los cuales afectan gravemente la confianza de los usuarios y comprometen la integridad de los sistemas bancarios. Además, el World Economic Forum (2024) informa que la ciberdelincuencia se ha convertido en una de las principales amenazas para la estabilidad financiera a nivel global, lo que ha impulsado a gobiernos y organismos internacionales a reforzar normativas y protocolos de seguridad.

En Perú, las instituciones bancarias han experimentado pérdidas considerables como resultado de ataques cibernéticos, con el 60% de las entidades financieras reportando al menos un incidente de seguridad en los últimos dos años (MINJUS, 2022). Este crecimiento en la frecuencia de los ataques evidencia la necesidad imperante de fortalecer las medidas de protección digital y de promover una mayor concienciación sobre los riesgos cibernéticos, tanto en los bancos como entre sus clientes (Veliz, 2023).

En Puno, la situación resulta igualmente preocupante, ya que el 25% de los usuarios bancarios en la región ha sido víctima de delitos cibernéticos en el último año, lo que ha debilitado la confianza en los servicios financieros. Además, las pequeñas y medianas empresas de Puno que operan con servicios bancarios en línea han reportado intentos de fraude digital o ataques cibernéticos (Aguilar, 2004). Estos hallazgos ponen de manifiesto una notable vulnerabilidad en la seguridad bancaria regional y destacan la necesidad urgente de implementar medidas más sólidas para proteger tanto

a los usuarios como a las instituciones financieras frente a las amenazas cibernéticas.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo se da la relación entre la impunidad de la ciberdelincuencia financiera y la vulneración a la seguridad bancaria, Puno 2024?

1.2.2. Problemas específicos

- PE1: ¿Cuál es el estado de la ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024?
- PE2: ¿Cuál es el estado de seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024?

1.3. Justificación

- **Justificación Teórica:**

  Este estudio es fundamental desde una perspectiva teórica porque se basó en la Teoría del Riesgo Percibido, el cual sostiene que la percepción del riesgo influye directamente en el comportamiento del consumidor. En el contexto de la banca en línea, la ciberdelincuencia financiera representa una amenaza tangible para los usuarios, quienes, al percibir una vulnerabilidad en la seguridad de sus transacciones, pueden modificar su comportamiento, reducir el uso de servicios digitales o perder confianza en las instituciones financieras.

- **Justificación Práctica:**

  En términos prácticos, este estudio ofrece soluciones directas para mejorar la seguridad bancaria y la confianza del cliente en los

servicios financieros en Puno. La ciberdelincuencia financiera no solo afecta las finanzas de los usuarios, sino también la reputación de las instituciones bancarias. Además, al identificar los principales factores de riesgo percibidos por los clientes y sus impactos en la confianza, este estudio proporcionará a los bancos información valiosa para reforzar sus sistemas de seguridad.

De la misma manera, los resultados servirán como una base para que las entidades financieras implementen mejores prácticas en ciberseguridad y desarrollen campañas de concientización dirigidas a sus usuarios sobre cómo protegerse contra el fraude digital.

- **Justificación Metodológica:**

  Para los fines de esta investigación, se utilizó una metodología cuantitativa, lo que permitió obtener información precisa y cuantificable sobre las opiniones de los clientes bancarios de Puno con respecto a los delitos cibernéticos relacionados con asuntos financieros. Se utilizó un cuestionario con escala Likert para recopilar datos representativos sobre la percepción del riesgo, la confianza en la seguridad de la banca y la influencia que la ciberdelincuencia tiene en el comportamiento de los usuarios. El examen estadístico de los datos permitió descubrir patrones y conexiones sustanciales entre las percepciones de la seguridad bancaria y el peligro percibido, lo que puede ser útil para construir modelos predictivos del comportamiento de los consumidores en caso de ciberdelincuencia.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Establecer la relación entre la impunidad de la ciberdelincuencia financiera y la vulneración a la seguridad bancaria, Puno 2024.

1.4.2. Objetivos específicos

- OE1: Identificar el estado de la ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024.
- OE2: Identificar el estado de seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024.

1.5. Hipótesis

1.5.1. Hipótesis general

La impunidad de la ciberdelincuencia financiera se relaciona significativamente con la vulneración a la seguridad bancaria, Puno 2024.

1.5.2. Hipótesis específicas

- HE1: Se tiene ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024.
- HE2: No se tiene seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024.

1.6. Operacionalización de variables

Tabla 1

Operacionalización de variables

Variable 1	Dimensiones	Indicadores	Ítems	Valores
1. Impunidad de la ciberdelincuencia financiera	1.1. tipos de delitos cibernéticos	1.1.1. Conocimiento de los delitos cibernéticos financieros	1, 2	a. Si. b. No.
		1.1.2. Frecuencia de ataques	3, 4	
	1.2. consecuencias de los ataques	1.2.1. Afectación de las cuentas bancarias	5, 6	
		1.2.2. Percepción del impacto financiero	7, 8	
Variable 2	**Dimensiones**	**Indicadores**	**Ítems**	**Valores**
2. Vulneración de la seguridad bancaria	2.1. Confianza en la seguridad bancaria	2.1.1. Nivel de confianza en la seguridad de las transacciones bancarias	9, 10	a. Si. b. No.
		2.1.2. Percepción de las medidas de seguridad	11, 12	
	2.2. Reacción ante un ataque cibernético	2.2.1. Procedimientos seguidos después de ser víctima de un ataque	13, 14	
		2.2.2. Satisfacción con las acciones del banco ante un ataque	15, 16	

Nota. La tabla ofrece un conjunto de términos que simplifican el análisis del tema investigado.

CAPÍTULO II

FUNDAMENTOS TEÓRICOS

2.1 Antecedentes de la investigación

2.1.1. A nivel internacional

En este contexto, Ojeda et al. (2020) Su trabajo se centró en el desarrollo de técnicas de gestión de riesgos para la Cooperativa de Ahorro y Crédito La Merced, con el objetivo de mejorar la seguridad de la información financiera y proteger los datos de los clientes. El enfoque utilizado fue descriptivo y no incluyó experimentación. Se utilizaron encuestas para obtener datos y se envió un cuestionario con dieciocho preguntas a diez trabajadores de los departamentos de contabilidad y riesgos. Los resultados revelaron que el veinticinco por ciento de los miembros que habían realizado transacciones electrónicas durante el último año se habían visto afectados, en su mayor parte, por ataques de phishing y malware. A medida que las instituciones financieras dependen cada vez más de la tecnología, se vuelven más vulnerables a las amenazas cibernéticas. Esta es la conclusión que se puede extraer del estudio realizado. Estos peligros podrían tener consecuencias catastróficas si no se toman las precauciones de seguridad suficientes. Por consiguiente, cualquier

institución financiera que desee llevar a cabo una transformación digital también debe realizar una inversión considerable en ciberseguridad y gestión de riesgos para superar los problemas a los que se enfrenta actualmente.

En su tesis, Teixido (2021) investigó los efectos del uso generalizado de la banca en línea en la ciberdelincuencia económica en el sistema financiero de la provincia de Mendoza durante la epidemia de COVID-19, que abarcó los años 2020 y 2021. El enfoque utilizado fue cuantitativo, descriptivo y de naturaleza no experimental. Los resultados del estudio indicaron que el phishing, especialmente el phishing realizado a través del correo electrónico, era el tipo de ciberdelincuencia más frecuente. Se produjo un aumento del 39 % en el número de estafas bancarias, un aumento del 29 % en las estafas con tarjetas de crédito y un aumento del 10 % en el número de estafas que utilizaban datos obtenidos a través de las redes sociales. Se llegó a la conclusión de que el aumento de los delitos cibernéticos ha superado las medidas de seguridad y las capacidades de gestión que se habían establecido anteriormente. con un 62% de las entidades bancarias enfrentando dificultades en la entrega de productos, gestión de consultas y reclamos, manejo de claves y cheques (PwC, 2021). El incremento en el uso del home banking y de aplicaciones bancarias ha llevado a una mejora en la capacitación del personal y a un fomento del trabajo remoto, permitiendo una continuidad en la atención. Este nuevo entorno ha provocado un cambio en el modus operandi del cibercrimen, adaptándose para explotar las oportunidades derivadas de la nueva normalidad actual.

En su tesis, Molina (2021) buscó analizar algunas políticas de ciberseguridad implementadas por las empresas del sector financiero en Colombia. La metodología utilizada fue de enfoque cuantitativo y nivel descriptivo, con una muestra compuesta por 500 personas, de las cuales se seleccionaron 60 de cinco entidades financieras distintas que manejan cuentas o productos del portafolio de estas empresas. Se utilizaron cuestionarios de opción múltiple para analizar los resultados. Según los resultados del estudio, el 56 % de los encuestados afirmó que prefiere realizar sus operaciones bancarias en persona, mientras que el 43 % indicó que prefiere hacerlo por Internet. Además, se concluyó que el 40% de la población no es consciente de los riesgos a los que está expuesta su información al realizar transacciones electrónicas, ni de que dicha información está bajo el control de las entidades financieras. De manera similar, una proporción significativa de usuarios desconoce la existencia de leyes estatales que protegen sus datos y garantizan la seguridad virtual.

2.1.2. A nivel nacional

Lopez (2023), Centraron los esfuerzos de su tesis en sugerir soluciones de seguridad bancaria que redujeran el número de incidentes de phishing que se producen en el sistema financiero y, como resultado, disminuyeran la probabilidad de que se violaran los derechos de los usuarios. Se utilizaron los procedimientos de archivo, análisis de documentos y observación como parte del enfoque cualitativo empleado. Las herramientas utilizadas comprendían archivos textuales y resúmenes, una guía de análisis de documentos y una guía de observación, entre otras. Los resultados indicaron que la detección de cuentas individuales y conjuntas de empleados

bancarios es la base de las técnicas de protección contra el fraude en los sistemas de información, además de la detección de hackers para garantizar que las operaciones financieras sean seguras y que correspondan a las transacciones habituales del usuario. En caso de una anomalía, se procede al bloqueo inmediato de la transacción. Concluye que, para proteger el patrimonio de los consumidores, el legislador peruano debe regular las medidas de seguridad bancaria, con un enfoque en respetar los derechos patrimoniales del consumidor y generar mecanismos preventivos para evitar el phishing.

En su tesis, Chilcon (2019) El objetivo principal era determinar el impacto que tienen los delitos cibernéticos en la seguridad nacional peruana. La investigación utilizó un enfoque cuantitativo y tuvo un diseño no experimental; su alcance fue descriptivo-explicativo. Participaron en la investigación un total de 231 personas, seleccionadas de la población estudiada, a quienes se les administró un cuestionario tipo Likert. Las hipótesis se validaron mediante la prueba de chi cuadrado. En comparación con otras técnicas de ciberdelincuencia en el país, los ataques informáticos son más comunes, según el 76,62 % de los encuestados. Sin embargo, el 12,99 % de los encuestados se opone a la idea de que se produzca tal efecto, y el 8,66 % no cree que exista. En conclusión, la investigación determinó que el cibercrimen en Perú tiene un impacto significativo en la seguridad nacional.

En su tesis, Flores (2023) El objetivo era investigar hasta qué punto las instituciones financieras son responsables de los delitos cibernéticos. El método utilizado fue una estrategia fundamental combinada. Los resultados

indican que el problema sigue agravándose por la lentitud del Gobierno peruano a la hora de actuar, no solo en lo que se refiere a la aplicación de medidas concretas, sino también al establecimiento de una legislación especializada y coherente en materia, como la creación de reglamentos y la adopción de las modificaciones necesarias. Se afirma que, en los últimos años, los delitos cibernéticos han aumentado drásticamente, y que el fraude informático, el robo de identidad y el tráfico ilícito de datos personales han cobrado especial relevancia en el sector financiero. Este crecimiento se ha producido en un entorno caracterizado por la pandemia, que ha provocado un cambio repentino en la forma en que las personas realizan su trabajo y participan en diversas actividades. Esto ha dado lugar a la modernización y al uso generalizado de la tecnología, especialmente en comparación con otros países.

2.1.3. A nivel local

En cuanto a la investigación local, no se encontraron estudios previos relevantes para los factores examinados en este estudio. Por lo tanto, este estudio tiene el potencial de servir como base y recurso para futuras investigaciones.

2.2.1. Teoría del riesgo percibido

La Teoría del Riesgo Percibido se centra en cómo los individuos perciben y evalúan los riesgos asociados con sus decisiones, especialmente en situaciones de incertidumbre. Esta teoría, desarrollada en el campo del comportamiento del consumidor, sugiere que las personas no siempre actúan basándose en el riesgo real, sino en el riesgo que perciben. La

percepción del riesgo puede estar influenciada por diversos factores, incluyendo experiencias previas, información disponible y la comunicación de la marca (Roselius, 1971). En esencia, la teoría destaca que los consumidores toman decisiones para minimizar su exposición a lo que perciben como riesgos potenciales.

En el contexto de la ciberdelincuencia financiera, la Teoría del Riesgo Percibido resulta relevante para entender cómo los clientes bancarios evalúan y responden a las amenazas cibernéticas. Los clientes que utilizan servicios de banca en línea pueden evaluar el riesgo percibido asociado con la posibilidad de ser víctimas de fraudes o pérdida de datos financieros. Esta percepción del riesgo puede influir en su disposición a adoptar o continuar usando servicios digitales de una institución bancaria (Lee & Lee, 2015). En lo que respecta a la aceptación y el uso continuado de los servicios de banca online, el nivel de confianza que tienen las personas en la seguridad de estos sistemas se está convirtiendo en un aspecto esencial.

Cuando ocurren incidentes de ciberdelincuencia, como ataques de phishing o ransomware, la percepción del riesgo entre los clientes puede aumentar significativamente. Un incidente de seguridad puede afectar negativamente la confianza de los clientes en la seguridad de los sistemas bancarios, haciendo que sean más reacios a utilizar servicios financieros digitales o incluso a cambiar de proveedor (Concepción et al., n.d.). Esto pone de manifiesto la importancia de una gestión adecuada de los incidentes de seguridad para mantener la confianza del cliente.

2.2.2. Impunidad de la ciberdelincuencia financiera

La ciberdelincuencia financiera se refiere a actividades delictivas que utilizan tecnologías de la información y la comunicación para cometer fraudes y otros delitos relacionados con el dinero y los servicios financieros (Kaspersky, 2024a). De acuerdo con UNODC (2022) la ciberdelincuencia financiera a menudo ocurre en entornos donde los delincuentes pueden operar de manera anónima. La dificultad para rastrear las transacciones digitales y la falta de recursos en las fuerzas del orden para investigar estos delitos contribuyen a un bajo riesgo de detección. Por otra parte, la desinformación sobre la ciberdelincuencia y sus consecuencias puede llevar a una falta de conciencia pública. Muchas personas no son plenamente conscientes de los riesgos asociados con las transacciones financieras en línea, lo que las hace más vulnerables a ataques como el phishing o el robo de identidad (Arapa et al., 2024).

2.2.2.1. Tipos de delitos cibernéticos.

De acuerdo con (Rextie, 2022), los delitos cibernéticos en el ámbito financiero incluyen varias categorías, entre las cuales se destacan:

- Phishing: Es un tipo de fraude en el que los delincuentes envían correos electrónicos o mensajes fraudulentos que parecen proceder de organizaciones financieras auténticas con el fin de engañar a los clientes para que revelen información confidencial, como contraseñas y datos de tarjetas de crédito (García, 2023).

- Malware: Este tipo de software malicioso se instala en los ordenadores de las víctimas con la intención de robar dinero, espiar sus actividades en Internet o bloquear el acceso a sistemas importantes hasta que se pague un rescate (López & Martínez, 2022).
- Ransomware: Similar al malware, el ransomware encripta los datos de la víctima y exige un pago para su liberación. En el ámbito financiero, esto puede significar la pérdida temporal de acceso a datos críticos o la interrupción de servicios (Pérez, 2023).
- Fraude en línea: Implica el uso de técnicas fraudulentas para engañar a las personas o instituciones, como la creación de sitios web falsos para recolectar información financiera (Ramos & García, 2021).

2.2.2.2. Consecuencias de los ataques.

Para Natalucci et al. (2024), los ataques cibernéticos en el sector financiero tienen consecuencias significativas tanto para las instituciones como para los clientes:

- Pérdidas económicas: Las instituciones financieras pueden sufrir pérdidas directas por el dinero robado, así como costos asociados con la mitigación del ataque, la reparación de sistemas y la compensación a clientes afectados (OEA, 2019).
- Daño a la reputación: La confianza de los clientes en una institución puede verse severamente afectada, lo que puede

llevar a una pérdida de clientes y una disminución en la base de usuarios (Kaspersky, 2024b)(Calle, 2022).

- Impacto en la seguridad de los datos: Los ataques pueden exponer datos personales y financieros sensibles, aumentando el riesgo de robos de identidad y otros tipos de fraudes (Kaspersky, 2024b).

2.2.3. La vulneración de la seguridad bancaria

El término “seguridad bancaria” hace referencia a los procedimientos y precauciones establecidos para proteger los datos financieros y las actividades bancarias de los consumidores frente a los ciberataques (Lévy et al., 2020).

La vulneración de la seguridad bancaria a menudo se manifiesta a través de ataques cibernéticos, como el phishing, malware y ransomware. Estos ataques buscan acceder a la información confidencial de los clientes, como contraseñas y datos bancarios, lo que puede resultar en robos de identidad y fraudes financieros (Por Redacción, 2024).

De acuerdo con Mamani (2024) la vulneración de la seguridad bancaria a menudo se relaciona con la mala gestión de datos y la falta de protocolos de protección adecuados. Esto puede incluir el uso de contraseñas débiles, la falta de cifrado de datos sensibles y la exposición de información personal a través de brechas de seguridad. Una gestión inadecuada de la información puede llevar a la filtración de datos sensibles, lo que permite a los delincuentes acceder a cuentas y realizar transacciones no autorizadas.

2.2.3.1. Confianza en la seguridad bancaria.

Según Cyber Security Global (2024) la confianza en la seguridad bancaria es crucial para el uso continuo de servicios financieros en línea. La percepción de seguridad por parte de los clientes se basa en:

- Medidas de protección:
  - Cifrado de datos: Protege la información sensible convirtiéndola en un formato ilegible para quienes no tengan la clave de descifrado.
  - Autenticación de múltiples factores (MFA): Requiere múltiples verificaciones para acceder a cuentas, añadiendo una capa de seguridad que dificulta el acceso no autorizado.
  - Sistemas de detección de fraudes: estos sistemas utilizan algoritmos sofisticados para detectar en tiempo real las transacciones que parecen fraudulentas. Esto permite reaccionar rápidamente ante comportamientos fraudulentos.
- Transparencia y comunicación:
  - Comunicación clara: Las instituciones deben informar proactivamente a los clientes sobre las medidas de seguridad adoptadas y cómo se gestionan los incidentes de seguridad.
  - Manejo de incidentes: Es crucial que, tras un incidente, las instituciones informen a los clientes sobre lo ocurrido y las

acciones correctivas tomadas para evitar futuros problemas.

- Educación continua: Invertir en la educación del cliente sobre ciberseguridad empodera a los usuarios y reduce su vulnerabilidad ante fraudes.

2.2.3.2. Reacción ante un ataque bancario.

Para Edigits (2021) la forma en que una institución financiera responde a un ataque cibernético puede afectar profundamente la percepción de su seguridad:

- Respuesta rápida y eficaz: La capacidad de respuesta ante un ciberataque debe ser casi instantánea. Esto implica contar con un plan de respuesta a incidentes bien definido y entrenar al personal en procedimientos específicos. Una reacción rápida no solo limita el daño causado por el ataque, sino que también reduce el tiempo de inactividad de los sistemas, lo que es vital para la operación continua del banco.
- Compensación a clientes: Las instituciones financieras deben tener equipos dedicados a la ciberseguridad que puedan evaluar la situación, identificar la naturaleza del ataque y tomar medidas adecuadas. Estos equipos, que suelen incluir expertos en tecnología y legalidad, son esenciales para realizar un análisis forense que ayude a entender el ataque y evitar que se repita.

2.3. Definición de términos

2.3.1. Impunidad

La impunidad se refiere a la ausencia, ya sea en la práctica o en el marco legal, de responsabilidad penal de quienes cometen violaciones, así como de las obligaciones civiles, administrativas o disciplinarias correspondientes. Esta situación se produce cuando los delincuentes logran eludir cualquier tipo de investigación que pueda dar lugar a su acusación, detención, juicio y, en caso de ser declarados culpables, a una pena adecuada, que puede incluir la indemnización por los daños causados a las víctimas (Consejo Económico y Social, 2005).

La falta de castigos no es el único factor que contribuye al concepto de impunidad; el término también se refiere a la ausencia de procesos judiciales e investigaciones contra las personas culpables de actividades delictivas. A las víctimas se les niega la oportunidad de conocer la verdad sobre lo ocurrido, identificar a los autores del delito y obtener una compensación adecuada por los daños que han sufrido como consecuencia de esta situación (Calvet, 2016).

Por otro lado, la impunidad representa la imposibilidad de enfrentar una sanción. Es una especie de excepción a la condena o un medio para eludir la justicia (Raffino, Equipo editorial, 2021).

2.3.2. Financiera

Para Prestamype (n.d.): "una institución financiera es similar a un banco en el sentido de que lleva a cabo actividades de intermediación financiera.

Esto implica que recoge los ahorros de la gente para llevar a cabo transacciones activas u otorgar créditos a terceros" (parr. 1).

Las instituciones financieras, por su parte, realizan transacciones con diversos valores, entre los que se incluyen acciones, bonos, letras de cambio, depósitos bancarios y otros instrumentos financieros (BBVA, 2024).

2.3.3. Vulneración

Para la RAE (2024) vulneración es : "Transgredir, quebrantar, violar una ley o precepto" (par. 1).

Según El Colegio de México (2024) la vulneración es el "Causar un daño grave o un perjuicio a la integridad de algo o alguien" (parr. 1).

CAPÍTULO III

METODOLOGÍA

3.1. Métodos de investigación

3.1.1. Enfoque de investigación

Cuantitativo:

El enfoque utilizado en esta investigación es el cuantitativo, que se caracteriza por su énfasis en el análisis de datos numéricos. Este tipo de enfoque permite llevar a cabo una evaluación objetiva y precisa de las variables estudiadas, facilitando la identificación de relaciones y patrones que pueden surgir entre diferentes fenómenos. Al utilizar técnicas estadísticas, el enfoque cuantitativo no solo proporciona una base sólida para la obtención de conclusiones, sino que también apoya el desarrollo y la validación de teorías en diversas disciplinas, desde las ciencias sociales hasta la economía y la psicología (Sabino, 1992).

3.1.2. Diseño de la investigación

No experimental:

Este estudio de investigación utilizó un diseño transversal no experimental, que se define por la observación y documentación de los acontecimientos tal y como se producen en su entorno natural, sin la participación directa

del investigador en la manipulación de variables o la administración de tratamientos experimentales (Sousa et al., 2007). Este tipo de diseño es especialmente útil en investigaciones donde el objetivo es obtener una visión instantánea de la situación de interés, permitiendo capturar la realidad en un momento específico.

3.1.3. Método

Hipotético deductivo:

Este estudio utilizó el método hipotético-deductivo como enfoque principal para examinar la relación entre la ciberdelincuencia financiera y la vulneración de la seguridad bancaria. Este método se fundamenta en la formulación de hipótesis que emergen de observaciones previas y teorías existentes sobre el fenómeno en cuestión, permitiendo así una investigación estructurada y sistemática (Marfull, 2019).

3.1.4. Tipo de investigación

Básico:

De acuerdo con Nicomendes (n.d.), el estudio, al ser de carácter básico, se distinguió por su capacidad para ahondar en la comprensión de fenómenos, abarcando tanto aspectos subjetivos como objetivos. Este enfoque es fundamental en la investigación básica, ya que busca no solo describir y analizar fenómenos, sino también entender las dinámicas que los subyacen.

3.1.5. Nivel de investigación

Explicativo:

Este estudio de investigación utiliza una técnica de investigación explicativa, que se caracteriza por su énfasis en identificar y analizar los efectos causales que se producen entre los fenómenos que se examinan. Como resultado, la investigación se centra en comprender mejor las formas en que los delitos cibernéticos pueden haber afectado a los clientes del Banco de Crédito del Perú (BCP) (Ramos, 2020).

3.2. Ámbito de investigación

El estudio de investigación se llevó a cabo en el distrito de Puno, una ciudad peruana situada en la región sur del país, en el altiplano de Collao. Puno es la capital del distrito, la provincia y el departamento que llevan el mismo nombre. En este contexto, el Banco de Crédito del Perú es el principal centro de atención.

Tabla 2

Ubicación geográfica del distrito de Puno

Población del Distrito Puno	129 922 hab.
Superficie	20.28 km²
Altitud	3819 m s. n. m.
Coordenadas geográficas	**Latitud:** 15°50′36″S
	Longitud: 70°01′25″O
Límites	**Norte:** Coata.
	Sur: Chucuito.
	Este: Lago Titicaca.
	Oeste: Paucarcolla.

Nota. La localización del distrito de Puno se basa en datos obtenidos de Wikipedia (2022).

3.3. Población y muestra

3.3.1. Población

Para el estudio, se seleccionó una población conformada por clientes que utilizan activamente los servicios ofrecidos por el Banco de Crédito del Perú en la ciudad de Puno. Esta muestra incluye usuarios frecuentes de los distintos canales de servicio bancario, como agencias físicas, banca por internet y aplicaciones móviles, con el fin de obtener una perspectiva amplia sobre las experiencias y desafíos en seguridad bancaria que enfrentan los usuarios.

3.3.2. Muestra

En cuanto a la muestra, se seleccionó una muestra compuesta por 29 clientes bancarios que hacen uso de los servicios del Banco de Crédito del Perú en Puno (Muntané, 2010).

a) Ser cliente activo del Banco de Crédito del Perú en Puno.
b) Tener al menos 18 años de edad.
c) Utilizar regularmente los servicios de banca digital (banca por internet, aplicación móvil).
d) Haber experimentado alguna vez problemas o situaciones relacionadas con la seguridad bancaria, como intentos de fraude o ciberataques.
e) Aceptar participar voluntariamente en el estudio y firmar el consentimiento informado.

Criterios de Exclusión:

a) No ser cliente del Banco de Crédito del Perú en Puno.
b) Menores de 18 años.

c) No utilizar los servicios de banca digital del banco.

d) Clientes que no deseen participar en el estudio o que no firmen el consentimiento informado.

e) Personas que presenten dificultades para responder adecuadamente debido a problemas de comunicación o comprensión del cuestionario.

3.3.3. Muestreo

El muestreo se realizó por conveniencia, seleccionando a las víctimas que se encontraban disponibles y dispuestas a participar en el estudio durante el periodo de recolección de datos.

3.4. Técnicas e instrumentos de recogida de información

3.4.1. Técnica

La técnica de encuesta es una herramienta fundamental en la investigación cuantitativa, ya que permite obtener información directa de los participantes sobre una variedad de temas relevantes. Según Carrasco (2006).esta metodología tiene varias ventajas que la hacen ideal para la recolección de datos en estudios sociales y de mercado.

3.4.2. Instrumentos

Se empleó un instrumento con escala LIKERT, diseñado para medir las percepciones y actitudes de los encuestados respecto a la seguridad bancaria y la ciberdelincuencia (Carrasco, 2006).

3.5. Recogida de datos

3.5.1. Confiabilidad

Según Oviedo & Campo (2005), La consistencia interna de un conjunto de ítems en un cuestionario o prueba se evalúa mediante el coeficiente alfa de Cronbach. Esto garantiza que las preguntas midan de

forma coherente el mismo concepto subyacente. Con el fin de determinar la fiabilidad del instrumento, en esta investigación se utilizó dicho coeficiente.

Tabla 3

Confiabilidad del estudio

Cuestionario	Ítems	Confiabilidad	Estado
Encuesta sobre la ciberdelincuencia financiera y la vulneración de la seguridad bancaria	16	0,79	Aceptable

Nota. La tabla muestra el nivel de confiabilidad alcanzado, que excede el límite de 0,70.

3.5.2. Validez de instrumento

Para verificar la validez de la investigación se utilizó el método del juicio de expertos, que consiste en que profesionales con amplios conocimientos sobre el tema evalúen el estudio. Escobar y Cuervo (2008) describen este método como una estrategia que implica la evaluación por parte de especialistas con amplios conocimientos sobre el tema. Estos profesionales, reconocidos por sus conocimientos y habilidades en la materia, aportaron comentarios, información y evaluaciones sustanciales sobre el instrumento.

CAPÍTULO IV

ANÁLISIS DE RESULTADOS Y DISCUSIÓN

4.1. Presentación

En este capítulo se analizan exhaustivamente los datos recopilados a partir de encuestas realizadas a una muestra de clientes del Banco de Crédito del Perú (BCP) en Puno. Esta investigación se lleva a cabo con el fin de comprender mejor la percepción que tienen los clientes sobre la seguridad en el sector bancario y el grado de eficacia que atribuyen a las medidas adoptadas por las entidades financieras frente a los delitos cibernéticos. Se aborda específicamente la relación entre la vulneración de la seguridad bancaria y la impunidad de los delitos cibernéticos financieros, considerando factores como el conocimiento de los usuarios sobre estos delitos, su confianza en las medidas de seguridad implementadas, y la satisfacción general frente a las respuestas y el apoyo ofrecidos por el banco ante incidentes cibernéticos.

Asimismo, se discuten las principales implicancias de estos hallazgos, analizando cómo la percepción de inseguridad y la experiencia de los clientes ante ataques cibernéticos pueden afectar la confianza y el uso de los servicios bancarios en línea.

4.2. Análisis e interpretación de resultados

4.2.1. Resultados de la variable 1 – impunidad de la ciberdelincuencia

Tabla 4

Dimensiones 1: tipos de delitos cibernético

Ítems	Valores				Total	
	Si		No			
	f	%	f	%	f	%
¿Está usted al tanto de los delitos cibernéticos financieros que afectan a los bancos?	19	65,5	10	34,5	29	100,0
¿Conoce usted algún tipo específico de delito cibernético financiero (por ejemplo, phishing, malware, etc.)?	18	62,1	11	37,9	29	100,0
¿Con qué frecuencia ha escuchado sobre ataques cibernéticos en el Banco de Crédito del Perú?	12	41,4	17	58,6	29	100,0
¿Ha experimentado personalmente o conoce a alguien que haya sufrido un ataque cibernético relacionado con su cuenta bancaria en el último año?	17	58,6	12	41,4	29	100,0

Nota. La tabla detalla los datos obtenidos de la encuesta aplicada a clientes bancarios del BCP.

Interpretación:

Los resultados de un estudio realizado en Puno entre veintinueve clientes del Banco de Crédito del Perú (BCP) se muestran en la Tabla 4. La encuesta constaba de cuatro preguntas que exploraban los conocimientos y experiencias de los participantes en materia de delitos cibernéticos relacionados con las finanzas.

Conocimiento general de los delitos cibernéticos financieros:

- El 65,5% de los encuestados (19 personas) respondió que está al tanto de los delitos cibernéticos que afectan a los bancos, mientras que el 34,5% (10 personas) indicó que no.

Conocimiento de tipos específicos de delitos (phishing, malware, etc.):

- Un 62,1% de los clientes (18 personas) reconoce algún tipo específico de delito cibernético financiero, frente a un 37,9% (11 personas) que no los identifica.

Frecuencia de conocimiento sobre ataques al BCP:

- Solo el 41,4% (12 personas) ha escuchado frecuentemente sobre ataques cibernéticos en el BCP, mientras que el 58,6% (17 personas) no ha oído hablar de ellos, lo que podría sugerir una percepción de baja incidencia o falta de difusión sobre estos eventos.

Experiencia personal o cercana con ataques cibernéticos:

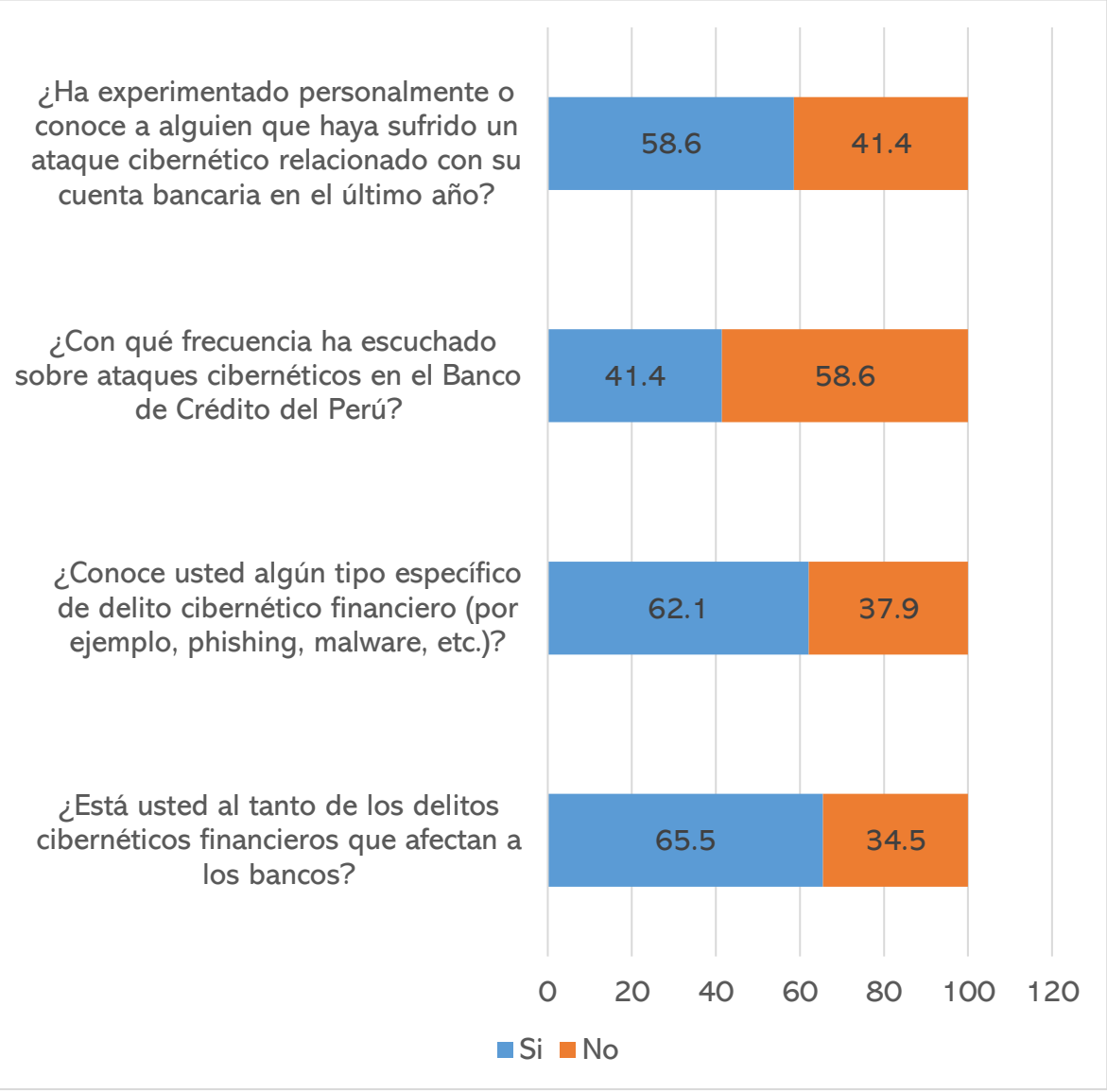
- El 58,6% de los encuestados (17 personas) ha experimentado personalmente o conoce a alguien que ha sido víctima de un ataque cibernético en su cuenta bancaria en el último año, mientras que el 41,4% (12 personas) no ha tenido esta experiencia.

En conjunto, estos datos indican que la mayoría de los clientes del BCP en Puno están al tanto de los delitos cibernéticos financieros y han experimentado o conocido casos de ciberataques. Sin embargo, más de la mitad desconoce los ataques específicos al BCP, lo que podría reflejar una falta de transparencia o comunicación sobre estos incidentes.

El resultado hallado tiene similitud con los siguientes estudios, según Mishima (2023) revela que los empleados de empresas en Arequipa reconocen la existencia de fraudes electrónicos y han escuchado sobre incidentes en sus organizaciones. No obstante, más del 60% de ellos no está familiarizado con las medidas de seguridad implementadas por su empresa para prevenir estos fraudes, lo que pone de manifiesto la urgencia de fomentar una cultura de seguridad cibernética dentro de las organizaciones.

Figura 1

Dimensiones 1: tipos de delitos cibernético



Nota. La figura representa la tabla 5.

Tabla 5

Dimensiones 2: consecuencias de los ataques

Ítems	Valores				Total	
	Si		No			
	f	%	f	%	f	%
¿Cree que los ataques cibernéticos han afectado la seguridad de las cuentas bancarias en su banco?	19	65,5	10	34,5	29	100,0
Si ha sido víctima de un ataque cibernético, ¿cómo afectó esto su cuenta bancaria?	12	41,4	17	58,6	29	100,0
¿Cuál considera que ha sido el impacto financiero de los ataques cibernéticos en los clientes del Banco de Crédito del Perú?	17	58,6	12	41,4	29	100,0
¿Cree que el impacto financiero de la ciberdelincuencia podría afectar su decisión de utilizar servicios bancarios en el futuro?	18	62,1	11	37,9	29	100,0

Nota. La tabla detalla los datos obtenidos de la encuesta aplicada a clientes bancarios del BCP.

Interpretación:

La Tabla 5 presenta los resultados de una encuesta aplicada a 29 clientes del Banco de Crédito del Perú (BCP) en Puno, abordando su percepción sobre las consecuencias de los ataques cibernéticos en el ámbito bancario.

Percepción sobre el impacto en la seguridad bancaria:

- El 65,5% de los encuestados (19 personas) cree que los ataques cibernéticos han afectado la seguridad de las cuentas bancarias en su banco, mientras que el 34,5% (10 personas) opina que no ha sido así. Esto

sugiere que una mayoría percibe una vulneración en la seguridad bancaria debido a los ataques.

Impacto directo en las cuentas bancarias de víctimas de ataques:

- Solo el 41,4% de los participantes (12 personas) que han sido víctimas de un ataque cibernético reporta que su cuenta bancaria se vio afectada, mientras que el 58,6% (17 personas) no ha experimentado un impacto directo. Esto puede indicar que, aunque la percepción de vulnerabilidad es alta, no todos los ataques resultan en consecuencias financieras directas para las víctimas.

Percepción del impacto financiero en clientes del BCP:

- El 58,6% de los encuestados (17 personas) considera que los ataques han tenido un impacto financiero significativo en los clientes del BCP, mientras que el 41,4% (12 personas) no comparte esta visión. Esto refleja una preocupación moderada sobre las consecuencias económicas de los ataques para los clientes en general.

Impacto en la decisión futura de uso de servicios bancarios:

- Un 62,1% de los encuestados (18 personas) cree que el impacto financiero de la ciberdelincuencia podría influir en su decisión de seguir utilizando servicios bancarios, en comparación con un 37,9% (11 personas) que no lo considera un factor decisivo. Esto sugiere que la seguridad cibernética influye en la confianza y en el uso futuro de servicios bancarios.

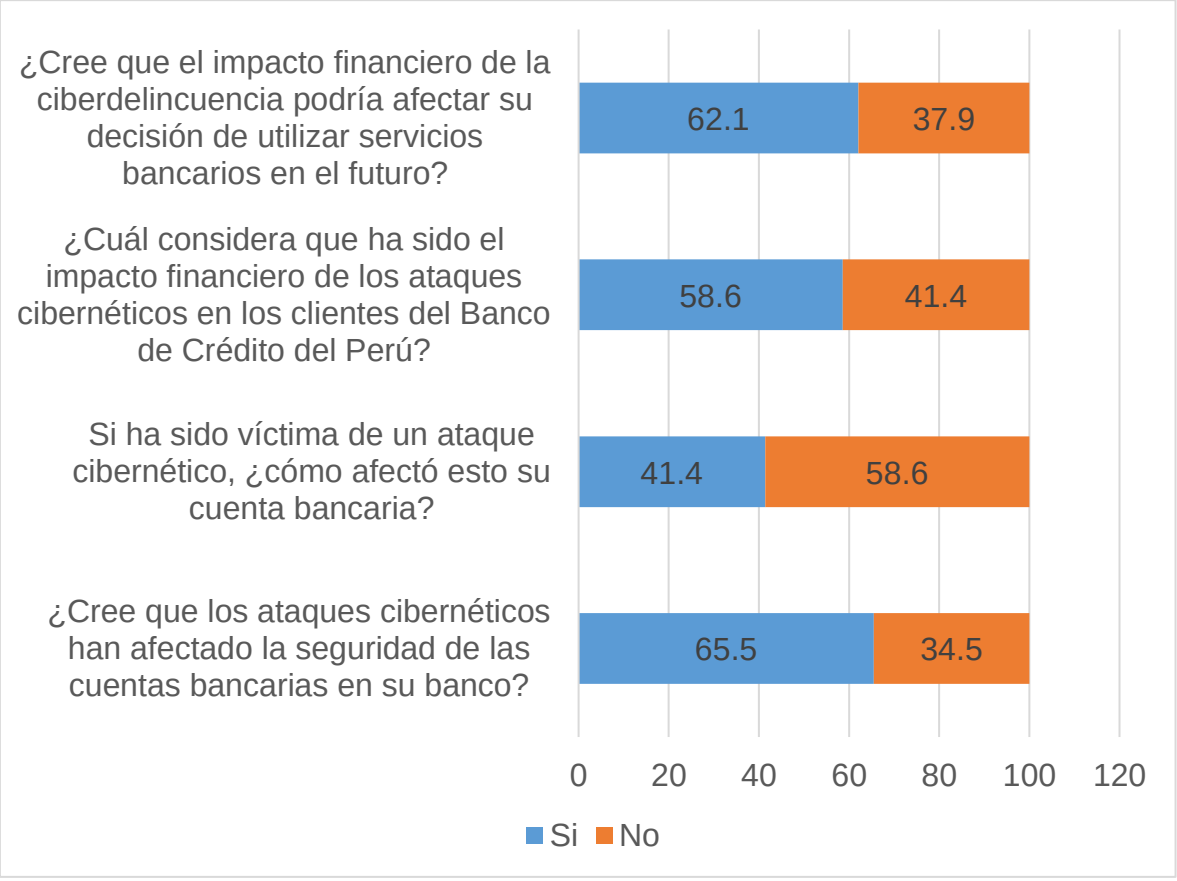
En resumen, los datos muestran que una mayoría de los clientes perciben que los ataques cibernéticos afectan la seguridad de las cuentas bancarias y tienen un

impacto financiero significativo, lo cual podría influir en su confianza y en su decisión de continuar utilizando servicios bancarios en el futuro.

El resultado se asemeja con lo mencionado por Kelly (2021) indican que una proporción significativa de los usuarios de servicios financieros reconoce la vulnerabilidad de sus cuentas ante ataques cibernéticos. Este sentimiento de inseguridad no solo afecta su percepción de la seguridad bancaria, sino que también tiene implicaciones directas en su disposición a utilizar productos financieros en el futuro. Asimismo, Perez (2015) señala que estos incidentes no solo comprometen la seguridad de sus cuentas, sino que también influyen en su decisión de seguir utilizando servicios ofrecidos por las instituciones bancarias.

Figura 2

Dimensiones 2: consecuencias de los ataques



Nota. La figura representa la tabla 5.

4.2.2. Resultados de la variable 2 – vulneración de la seguridad bancaria

Tabla 6

Dimensiones 1: confianza en la seguridad bancaria

Ítems	Valores				Total	
	Si		No			
	f	%	f	%	f	%
¿Qué tan seguro se siente al realizar transacciones bancarias en línea?	12	41,4	17	58,6	29	100,0
¿Confía en que el Banco de Crédito del Perú tiene medidas adecuadas para proteger sus transacciones en línea?	10	34,5	19	65,5	29	100,0
¿Cómo calificaría las medidas de seguridad implementadas por su banco para proteger a los clientes de ciberdelincuencia?	11	37,9	18	62,1	29	100,0
¿Está informado sobre las medidas de seguridad que su banco implementa para proteger sus datos personales y financieros?	12	41,4	17	58,6	29	100,0

Nota. La tabla detalla los datos obtenidos de la encuesta aplicada a clientes bancarios del BCP.

Interpretación:

La Tabla 6 presenta los resultados de una encuesta realizada a 29 clientes del Banco de Crédito del Perú (BCP) en Puno, enfocándose en la confianza de los usuarios en la seguridad bancaria.

Confianza en la seguridad de las transacciones en línea:

- Solo el 41,4% de los encuestados (12 personas) se siente seguro al realizar transacciones bancarias en línea, mientras que el 58,6% (17 personas) no

se siente seguro. Esto sugiere una baja percepción de seguridad en las operaciones bancarias digitales.

Confianza en las medidas de protección del BCP:

- Apenas el 34,5% de los clientes (10 personas) confía en que el BCP cuenta con medidas adecuadas para proteger sus transacciones en línea, mientras que el 65,5% (19 personas) no confía en estas medidas. Esto indica una percepción generalizada de insuficiencia en las estrategias de seguridad del banco.

Evaluación de las medidas de seguridad del banco:

- Las medidas de seguridad establecidas por el banco para proteger a sus clientes contra los delitos informáticos son valoradas positivamente por el 37,9 % de los encuestados (11 personas), mientras que el 62,1 % (18 personas) considera que estas medidas no son suficientes. Esto refleja que la mayoría de las personas tiene una opinión desfavorable sobre la eficacia de las prácticas de seguridad del banco.

Conocimiento sobre las medidas de seguridad del banco:

- El 41,4% de los clientes (12 personas) está informado sobre las medidas de seguridad implementadas por el BCP para proteger sus datos personales y financieros, mientras que el 58,6% (17 personas) no está al tanto de estas medidas. Esto podría indicar una falta de comunicación o difusión adecuada por parte del banco sobre sus políticas de seguridad.

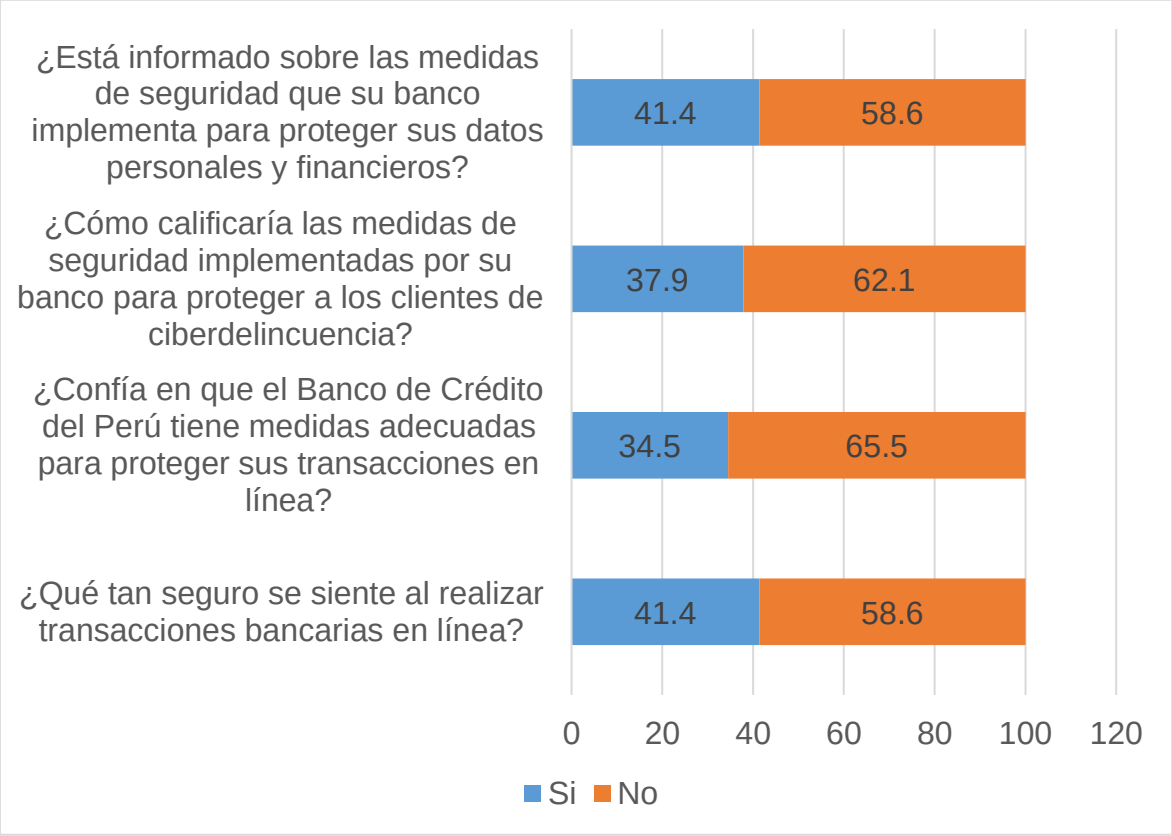
En resumen, los resultados muestran una baja confianza y conocimiento entre los clientes del BCP en Puno respecto a la seguridad de las transacciones en línea y

las medidas de protección del banco frente a la ciberdelincuencia. La mayoría de los clientes percibe las medidas de seguridad como insuficientes, lo cual podría afectar la confianza en la institución.

El resultado se asemeja con lo mencionado por, Gonzales (2018) revelan que los clientes del Banco de Crédito del Perú en Puno presentan un nivel de desconfianza y escaso conocimiento sobre las medidas de seguridad implementadas para proteger sus transacciones en línea. Para El Peruano (2020) indica que existe una significativa falta de confianza y comprensión entre los clientes del BCP en Puno respecto a las medidas de seguridad que protegen sus transacciones en línea. La mayoría de los usuarios considera que las iniciativas del banco son insuficientes para enfrentar la ciberdelincuencia.

Figura 3

Dimensiones 1: confianza en la seguridad bancaria



Nota. La figura representa la tabla 5.

Tabla 7

Dimensiones 2: Reacción ante un ataque cibernético

Ítems	Valores				Total	
	Si		No			
	f	%	f	%	f	%
Si ha sido víctima de un ataque cibernético, ¿qué medidas tomó para reportar el incidente?	10	34,5	19	65,5	29	100,0
¿Cuán efectivo considera que fue el procedimiento seguido por su banco tras un ataque cibernético?	11	37,9	18	62,1	29	100,0
¿Está satisfecho con la respuesta de su banco después de un ataque cibernético?	12	41,4	17	58,6	29	100,0
¿Considera que su banco proporciona suficiente apoyo y asesoramiento a los clientes que han sido víctimas de ciberdelincuencia?	11	37,9	18	62,1	29	100,0

Nota. La tabla detalla los datos obtenidos de la encuesta aplicada a clientes bancarios del BCP.

Interpretación:

La Tabla 7 presenta los resultados de una encuesta realizada a 29 clientes del Banco de Crédito del Perú (BCP) en Puno sobre su reacción y satisfacción con la respuesta del banco ante un ataque cibernético.

Medidas para reportar el incidente:

- El 34,5% de los encuestados (10 personas) tomó medidas para reportar el incidente tras ser víctima de un ataque cibernético, mientras que el 65,5% (19 personas) no lo hizo. Esto sugiere que una mayoría no reporta estos

incidentes, lo cual puede deberse a factores como falta de información sobre los procedimientos o desconfianza en la efectividad de los mismos.

Efectividad del procedimiento del banco:

- Solo el 37,9% de los clientes (11 personas) considera que el procedimiento seguido por el banco tras un ataque cibernético fue efectivo, en contraste con el 62,1% (18 personas) que lo evalúa como inefectivo. Esto refleja una percepción negativa sobre la capacidad del banco para manejar incidentes de seguridad de manera adecuada.

Satisfacción con la respuesta del banco:

- El 41,4% de los encuestados (12 personas) está satisfecho con la respuesta del banco después de un ataque cibernético, mientras que el 58,6% (17 personas) no está satisfecho. Esto sugiere que la mayoría de los clientes perciben la respuesta del banco como insuficiente o inadecuada para sus necesidades tras un incidente de seguridad.

Apoyo y asesoramiento del banco:

- Solo el 37,9% de los clientes (11 personas) considera que el banco proporciona suficiente apoyo y asesoramiento a las víctimas de ciberdelincuencia, mientras que el 62,1% (18 personas) opina lo contrario. Esto indica una percepción general de que el banco no brinda el acompañamiento necesario para los afectados por ciberdelitos.

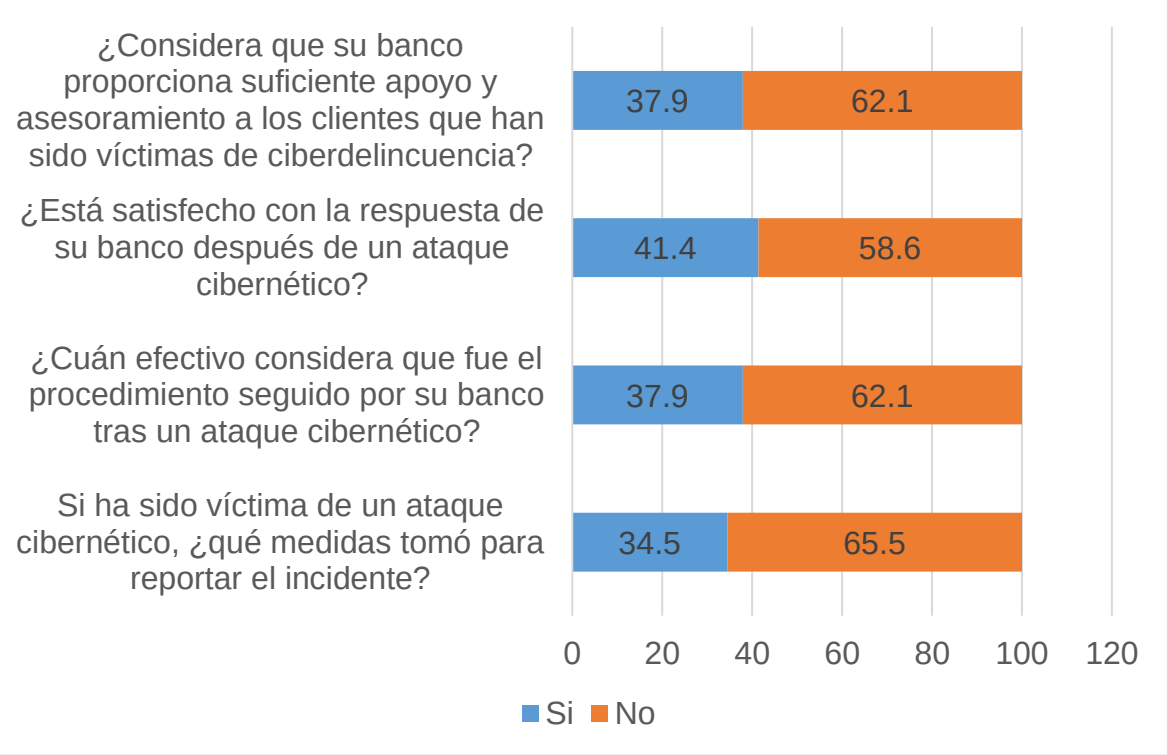
En resumen, los datos reflejan una baja satisfacción entre los clientes con respecto a la respuesta del BCP ante ataques cibernéticos. La mayoría percibe los procedimientos como ineficaces y siente que el banco no ofrece el apoyo necesario

tras ser víctimas de ciberdelincuencia, lo cual puede influir en la confianza y lealtad hacia la institución bancaria.

El resultado se asemeja con lo hallado por Natalucci et al. (2024) muestran una insatisfacción considerable con la manera en que la entidad gestiona su respuesta a los ataques cibernéticos. La falta de asistencia tras los incidentes de ciberdelincuencia y la idea de que los procesos establecidos no son eficaces indican que estos inconvenientes pueden tener un impacto negativo en la confianza y la lealtad de los clientes hacia la institución financiera. Además, Único punto de contacto digital del Estado Peruano con los ciudadanos (2024)concluye que la mayoría de los clientes del BCP expresan una insatisfacción significativa con la respuesta del banco ante ciberataques, considerándola ineficaz y carente del apoyo necesario para quienes han sido víctimas.

Figura 4

Dimensiones 2: Reacción ante un ataque cibernético



Nota. La figura representa la tabla 5.

4.3. Prueba de hipótesis

Se empleó el coeficiente rho de Spearman para la comprobación de hipótesis. El coeficiente rho de Spearman es un coeficiente de correlación no paramétrico que indica la fuerza y la dirección del vínculo entre dos variables ordinales.

La fórmula para calcular el rho de Spearman (ρs) es:

$$\rho_s = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)}$$

Interpretación:

- Un ρs de +1 indica una correlación perfecta positiva (los rangos de ambas variables aumentan juntos).
- Un ρs de -1 indica una correlación perfecta negativa (un aumento en una variable está asociado con una disminución en la otra).
- Un ρs de 0 indica que no hay correlación entre las variables.

Hg: La ciberdelincuencia financiera se relaciona significativamente con la vulneración a la seguridad bancaria, Puno 2024.

- **Ha:** La ciberdelincuencia financiera se relaciona significativamente con la vulneración a la seguridad bancaria, Puno 2024.
- **H0:** La ciberdelincuencia financiera no se relaciona significativamente con la vulneración a la seguridad bancaria, Puno 2024.

Tabla 8

Correlación de la hipótesis general

			Ciberdelincuencia financiera	Vulneración de la seguridad bancaria
Rho de Spearman	Ciberdelincuencia financiera	Coeficiente de correlación	1,000	0,678**
		Sig. (bilateral)	.	0,000
		N	29	29
	Vulneración de la seguridad bancaria	Coeficiente de correlación	0,678**	1,000
		Sig. (bilateral)	0,000	.
		N	29	29

**. La correlación es significativa en el nivel 0,01 (2 colas).

Nota. La tabla muestra los resultados hallados de la aplicación de la prueba de RHO.

Interpretación:

Los resultados de la prueba de hipótesis, que se llevó a cabo utilizando el coeficiente de correlación de Spearman para evaluar la asociación entre los delitos cibernéticos financieros y las violaciones de seguridad en las instituciones bancarias, se muestran en la tabla.

El coeficiente de correlación de Spearman entre la ciberdelincuencia financiera y la vulneración de la seguridad bancaria es 0.678, lo que indica una correlación positiva y moderadamente alta. Este valor sugiere que a medida que aumentan los casos de ciberdelincuencia financiera, también se incrementa la vulneración de la seguridad bancaria.

El valor de significancia (Sig.) es 0.000, lo que es inferior al nivel de significancia establecido de 0.01. Esto indica que la correlación observada es estadísticamente significativa.

En efecto, se rechaza la hipótesis nula (H0), lo que confirma que la ciberdelincuencia financiera se relaciona significativamente con la vulneración a la seguridad bancaria en Puno, 2024.

4.4. Discusión de resultados

En este punto, se interpretarán los resultados obtenidos en el estudio, analizando su relevancia en el contexto de la seguridad bancaria en el Banco de Crédito del Perú (BCP) en Puno, y relacionándolos con la literatura existente sobre el tema.

Respecto al primer objetivo: Identificar el estado de la ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024. Los resultados del estudio indican que la seguridad bancaria en el BCP enfrenta serios desafíos relacionados con la ciberdelincuencia. Este presenta un estado elevado de ciberdelincuencia. Respecto a la discusión sobre el estado de la ciberdelincuencia en el BCP de Puno revela una percepción generalizada de insuficiencia en las medidas de seguridad bancaria, similar a lo identificado en estudios previos. Además, Ojeda et al. (2020) y Teixido (2021) destacaron el aumento de amenazas como el phishing y la vulnerabilidad del sistema financiero, lo cual es congruente con la percepción de riesgo de los clientes del BCP en Puno. Además, Flores (2023) y López (2023) subrayan la necesidad de mejorar tanto la regulación como la respuesta ante ataques cibernéticos en Perú, coincidiendo con los

hallazgos de este estudio, que sugieren una inversión en ciberseguridad y mejores protocolos de protección y apoyo al cliente en caso de ciberataques.

En cuanto al segundo objetivo: Identificar el estado de seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024. la discusión de los resultados resalta que el estado de la seguridad bancaria en el BCP en Puno refleja tendencias observadas en otras instituciones, tanto a nivel nacional como internacional. En cuanto al análisis de seguridad bancaria en el BCP de Puno revela desafíos compartidos con otras instituciones financieras, especialmente en la prevención de ataques como phishing y malware. Ojeda et al. (2020) y Teixido (2021) subrayan la vulnerabilidad derivada del uso de plataformas digitales y la limitada respuesta ante amenazas cibernéticas. Además, López (2023) y Flores (2023) enfatizan la necesidad de políticas robustas y regulaciones específicas para proteger los datos de los usuarios. En conjunto, estos estudios destacan la importancia de fortalecer la ciberseguridad en el BCP para afrontar eficazmente los riesgos actuales en el sector financiero.

CONCLUSIONES

PRIMERA. – Se determinó que los delitos cibernéticos financieros están estrechamente relacionados con las violaciones de la seguridad bancaria, Puno 2024. Una prueba Rho arrojó un resultado de 0,678, acompañado de un valor p de 0,000 ($p<0,05$), lo que indica que el aumento de los delitos cibernéticos financieros se correlaciona con una disminución de la seguridad bancaria (correlación inversa).

SEGUNDA. – Se identifico que se tiene ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024. Esto se evidencia por la falta de conocimiento sobre los delitos cibernéticos financieros en el 65,5% de los encuestados y por un incremento en la percepción de ataques frecuentes, reportado por el 58,6%. Asimismo, el 65,5% de los participantes confirmó haber sido víctima de un ataque cibernético que afectó sus cuentas bancarias, lo que resalta la vulnerabilidad de la entidad frente a estos delitos.

TERCERA. – Se identifico que no se tiene seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024. Esto se refleja en la baja confianza en la seguridad de las transacciones bancarias, donde el 58,6% de los encuestados manifestó desconfianza, y una percepción negativa hacia las medidas de seguridad implementadas, también del 58,6%. Además, el 65,5% de los clientes reportó que el banco no brindó un apoyo adecuado tras haber sido víctimas de ataques cibernéticos, lo que pone en evidencia una deficiente respuesta ante estas situaciones.

RECOMENDACIONES

PRIMERA. – Al presidente del consejo de administración del Banco de Crédito del Perú: con el fin de identificar y prevenir los ciberataques, se deben implementar tecnologías más modernas, como sistemas de inteligencia artificial para la supervisión continua de posibles amenazas y la identificación de patrones anómalos.

SEGUNDA. – Al presidente del directorio del Banco de Crédito del Perú, a que implementen programas educativos permanentes para capacitar tanto a sus empleados como a los usuarios sobre los tipos de ciberdelitos, sus riesgos, y las mejores prácticas de seguridad. Estos programas pueden incluir talleres presenciales, campañas informativas, y recursos online.

TERCERA. – A la Superintendenta de Banca, Seguros y AFP, a que debería intensificar la supervisión de las políticas de seguridad cibernética en los bancos del país, especialmente en áreas vulnerables como Puno, y aplicar sanciones o directrices específicas para mejorar las respuestas bancarias a las brechas de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, M. (2004). *El financiamiento, de las micro y pequeñas empresas en puno. un análisis empírico de la demanda de créditos*. https://cies.org.pe/wp-content/uploads/2014/03/el-financiamiento-de-las-micro-y-pequenas-empresas-en-puno-un-analisis-empirico-de-la-demanda-de-creditos.pdf

Arapa, J., Cari, K., & Laura, J. (2024). Causas y consecunecias del incremento de los delitos informaticos en la ciudad de Puno 2023. *Redalyc*. https://www.redalyc.org/journal/6718/671876168004/index.html

Arnal, C. (2024). *Cómo elevar la ciberseguridad de las compañías financieras*. Watchguard.Com. https://www.watchguard.com/es/wgrd-news/blog/como-elevar-la-ciberseguridad-de-las-companias-financieras-0

BBVA. (2024). *¿Qué son las inversiones financieras y qué tipos existen?* Bbva.Com. https://www.bbva.com/es/salud-financiera/que-es-una-tarjeta-de-debito-y-como-puedo-usarla/

Calle, J. (2022). *4 riesgos que pueden afectar la reputación de tu empresa*. https://www.piranirisk.com/es/blog/4-riesgos-que-pueden-afectar-la-reputacion-de-su-empresa

Calvet, E. (2016). Impunidad (ausencia de castigo). *Eunomía. Revista En Cultura de La Legalidad*, *10*, 144–157. https://e-revistas.uc3m.es/index.php/EUNOM/article/view/3054/1751

Carrasco, S. (2006). *Metódologia de la investigación científica*. Editorial San Marcos.

Chilcon, S. (2019). *El Cibercrimen En El Peru Y Su Incidencia En La Seguridad Nacional* [Centro de Altos Estudios Nacionales].

https://repositorio.caen.edu.pe/server/api/core/bitstreams/42570992-50ff-4c72-81cc-6bf57beff4d8/content

Concepción, N., Vásquez, R., & Iglesias, V. (n.d.). *Consumidores bancarios: emociones, valoraciones cognitivas y satisfacción ante fallos y recuperaciones de servicio*. https://www.aemarkcongresos.com/congreso2007/comportamiento/cc10-p.pdf

Consejo Económico y Social. (2005). *Informe de Diane Orentlicher, experta independiente encargada de actualizar el conjunto de principios para la lucha contra la impunidad*.

Cyber Security Global. (2024). *Ciberseguridad Bancaria: ¿Cómo Proteger los Activos Financieros Digitales?* Cyber-Security.Global. https://cyber-security.global/ciberseguridad-bancaria-como-proteger-los-activos-financieros-digitales/

Edigits. (2021). *Fortalezas y desafios de ciberseguridad en el s ecto financiero*. Www.3digits.Es. https://www.3digits.es/blog/ciberseguridad-en-el-sector-financiero.html

El Colegio de México. (2024). *vulnerar*. Dem.Colmex.Mx. https://dem.colmex.mx/ver/vulnerar

El Peruano. (2020). *Sancionan al BCP por no resguardar la confidencialidad de datos personales de clientes*. Elperuano.Pe. https://www.elperuano.pe/noticia/103884-sancionan-al-bcp-por-no-resguardar-la-confidencialidad-de-datos-personales-de-clientes

Escobar, J., & Cuervo, A. (2008). Validez de contenido y juicio de expertos: una

aproximación a su utilización. *Avances En Medición,* 27–36. http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf

ESENTIRE. (2024). *Cybersecurity Ventures Report on Cybercrime*. Esentire.Com. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime

Flores, C. (2023). *La responsabilidad de las entidades financieras ante la comisión de delitos informáticos* [Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/27260/FLORES_JIMENEZ_CARLOS_ARTURO.pdf?sequence=1&isAllowed=y

García, J. (2023). Algunas consideraciones sobre la reforma del delito de malversación y la protección penal del patrimonio público. *Documentación Administrativa*, 59–72. https://doi.org/10.24965/da.11210

Gobierno Digital. (2024). *El Indecopi inició investigación preliminar al BCP ante reclamos reportados por usuarios por problemas en sus canales de pago*. Gob.Pe. https://www.gob.pe/institucion/indecopi/noticias/998992-el-indecopi-inicio-investigacion-preliminar-al-bcp-ante-reclamos-reportados-por-usuarios-por-problemas-en-sus-canales-de-pago

Gonzales, M. (2018). *Plan estratégico para el agente BCP del Banco de Credito del Peru 2014-2017* [Universidad del Pacifico]. https://repositorio.up.edu.pe/bitstream/handle/11354/2038/Miguel_Tesis_maestria_2018.pdf?sequence=1

Kaspersky. (2024a). *¿Qué es el cibercrimen? Cómo protegerse del cibercrimen*. Latam.Kaspersky.Com. https://latam.kaspersky.com/resource-

center/threats/what-is-cybercrime?srsltid=AfmBOoruW7zNmMhibBKROhsQBO4Bx3fVMp78ayABoN4MFJ1NkFoSAoDf

Kaspersky. (2024b). *¿Qué es el robo de datos y cómo evitarlo?* Latam.Kaspersky.Comkaspersky. https://latam.kaspersky.com/resource-center/threats/data-theft?srsltid=AfmBOoqVBhkaHBSAWZzhyAgzCYIlVi--hPC_fQ5Rt-xbnmYSbbq7yLIW

Kelly, B. (2021). *Amenazas de seguridad en los servicios financieros*. Globalsign.Com. https://www.globalsign.com/es/blog/5-friday-5-security-threats-facing-financial-services-industry

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises. *Business Horizons*, *58*, 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lévy, J., Bourgault, N., Calvo, C., & Trudel, M. (2020). La influencia de la confianza y satisfacción del cliente en la intención de uso de los servicios bancarios por internet: un modelo estructural. *Revista Científica Multidisciplinaria de Prospectiva*, *27*(2). https://www.redalyc.org/journal/104/10462656003/html/

Lopez, H. (2023). *Medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero* [Universidad Católica Santo Toribio de Mogrovejo]. https://tesis.usat.edu.pe/bitstream/20.500.12423/6891/1/TL_LopezOcampoHuillari.pdf

Mamani, E. (2024). *Ciberseguridad y vulneración de datos personales en*

entidades financieras. Lpderecho.Pe. https://lpderecho.pe/ciberseguridad-vulneracion-datos-personales-entidades-financieras/

Marfull Pujadas, A. (2019). *El método hipotético-deductivo de Karl Popper*. Andreumarfull.Com. https://andreumarfull.com/2019/12/18/el-metodo-hipotetico-deductivo/

MINJUS. (2022). *Ciberdelincuencia Reporte De Información Estadística Y Recomendaciones Para La Prevención*. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte de Ciberdelincuencia.pdf.pdf

Mishima, M. (2023). *EY: 40% de compañías en Perú registra incidentes críticos de ciberseguridad*. Ey.Com. https://www.ey.com/es_pe/news/2023/01/companias-peru-incidentes-ciberseguridad

Molina, S. (2021). *Ciberseguridad de las empresas financieras* [Tecnológico de Antioquia Institución Universitaria]. https://dspace.tdea.edu.co/bitstream/handle/tdea/2307/49. TGII Ciberseguridad en las empresas financieras.pdf?sequence=1&isAllowed=y

Muntané, J. (2010). Introducción a la investigaciòn básica. *Revista Andaluza de Patología Digestiva*, *33*(3), 221–227.

Natalucci, F., Mahvash, Q., & Suntheim, F. (2024). *Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera*. Imf.Org. https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability#:~:text=Sin ir más lejos%2C un,mercado e incluso corridas bancarias.

Nicomendes, E. (n.d.). *Tipos de investigación*. https://core.ac.uk/download/pdf/250080756.pdf

OEA. (2014). *Tendencias de Seguridad Cibérnetica en America Latina y el Caribe*. 100. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014 - Tendencias de Seguridad Cibernética en América Latina y el Caribe.pdf

OEA. (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe*. *1*, 1–182. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

OEA. (2019). *Desafios del riesgo cibernético en el sector financiero para Colombia y America latina*. Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Ojeda, F., Moreno, V., & Torres, M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *Cienciamatria*, *6*(2), 192–219. https://doi.org/10.35381/cm.v6i2.366

Oviedo, H., & Campo, A. (2005). Metodología de investigación y lectura critica de estudios: Aproximación al uso del coeficiente alfa de Cronach. *Revista Colombiana de Psiquiatria*, *XXXIV*(4). https://doi.org/10.1590/s1135-57272002000200001

Perez, J. (2015). *Análisis de la banca por internet entre los usuarios particulares. Un modelo en dinámica de sistemas* [Universidad de Valladolid]. https://uvadoc.uva.es/bitstream/handle/10324/14079/tesis707-151005.pdf?sequence=1

Por Redacción. (2024). *¿Cuáles son los principales desafíos de seguridad en el sector bancario?* Segurilatam.Com. https://www.segurilatam.com/actualidad/seguridad-en-el-sector-bancario-principales-desafios_20240730.html

Prestamype. (n.d.). *¿Qué es una financiera?* Prestamype.Com. https://www.prestamype.com/articulos/que-es-una-financiera

RAE. (2024). *vulnerar*. Dle.Rae.Es. https://dle.rae.es/vulnerar

Raffino, Equipo editorial, E. (2021). *Impunidad*. Concepto.De. https://concepto.de/impunidad/

Ramos, C. A. (2020). Alcances de una investigación. *CienciAmérica*, *9*(3), 1–6. https://doi.org/10.33210/ca.v9i3.336

Rextie. (2022). *Los tipos de delitos informáticos más recurrentes que amenazan a las empresas*. Rextie.Com. https://www.rextie.com/blog/6-modalidades-mas-recurrentes-de-delitos-informaticos/

Roselius, T. (1971). Consumer rankings of risk reduction methods. *Journal of Marketing*, *35*(1), 56–61. https://doi.org/10.2307/1250565

Sabino, C. (1992). *El proceso de investigación* (Panapo (ed.)). Editorial Panamericana.

Sousa, V., Driessnack, M., & Costa, I. (2007). Revisión de diseños de investigación resaltantes para enfermería. Parte1: Diseño de investigación cuantitativa. *Revista Latinoamericana Enfermagem*, *15*(3), 6. https://www.scielo.br/j/rlae/a/7zMf8XypC67vGPrXVrVFGdx/?format=pdf&lang=es

Teixido, E. (2021). *Ciberdelito y vulnerabilidad del Sistema Bancario en la*

provincia de Mendoza [Instituto Universitario de Seguridad Pública]. https://bdigital.uncuyo.edu.ar/objetos_digitales/18493/teixido-ciberdelito.pdf

UNODC. (2022). *Compendio De Ciberdelincuencia Organizada*. Naciones Unidas. https://www.unodc.org/documents/Cybercrime/tools-and-resources/compendio_de_delincuencia_organizada_es.pdf

Veliz, J. (2023). *Ciberdelincuencia e Inteligencia Artificial ¿Puede el Perú defenderse ante estas amenazas digitales?* Rpp.Pe. https://rpp.pe/tecnologia/mas-tecnologia/ciberdelincuencia-e-inteligencia-artificial-en-peru-2023-noticia-1508418#:~:text=En 2023%2C Perú enfrenta una,significativos para la seguridad digital.

Wikipedia. (2022). *Departamento de Puno*. Wikipedia.Org. https://es.wikipedia.org/wiki/Departamento_de_Puno

World Economic Forum. (2024). The Global Risks Report 2024. In *Economic and Political Weekly* (Vol. 59, Issue 9). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

APÉNDICE

Apéndice 1 Matriz de Consistencia

Título de la investigación: VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024						
Investigador (a): KATIA FIORELA APAZA FLORES						
Problema	**Objetivos**	**Hipótesis**	**Variables**	**Dimensiones**	**Indicadores**	**Metodología**
Problema general	**Objetivo general**	**Hipótesis general**	Variable 1: Impunidad de la ciberdelincuencia financiera Variable 2: Vulneración de la seguridad bancaria	Tipos de delitos cibernéticos Consecuencias de los ataques Confianza en la seguridad bancaria Reacción ante un ataque cibernético	Conocimiento de los delitos cibernéticos financieros Frecuencia de ataques Afectación de las cuentas bancarias Percepción del impacto financiero Nivel de confianza en la seguridad de las transacciones bancarias Percepción de las medidas de seguridad Procedimientos seguidos después de ser víctima de un ataque Satisfacción con las acciones del banco ante un ataque	Enfoque: cuantitativo. Método: hipotético deductivo. Tipo: básico. Nivel: descriptivo. Diseño: no experimental. Población: clientes del Banco de Crédito del Perú de Puno. Muestra: 29 clientes bancarios que utilizan el servicio del Banco de Crédito del Perú de Puno. Muestreo: por conveniencia, no probabilístico. Técnica e instrumentos: encuesta y cuestionario dicotómico.
P.G. ¿Cómo se da la relación entre la impunidad de la ciberdelincuencia financiera y la vulneración a la seguridad bancaria, Puno 2024?	O.G. Establecer la relación entre la impunidad de la ciberdelincuencia financiera y la vulneración a la seguridad bancaria, Puno 2024.	H.G. La impunidad de la ciberdelincuencia financiera se relaciona significativamente con la vulneración a la seguridad bancaria, Puno 2024.				
Problemas Específicos	**Objetivos específicos**	**Hipótesis específicas**				
P.E.1. ¿Cuál es el estado de la ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024?	O.E.1. Identificar el estado de la ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024.	H.E.1. Se tiene ciberdelincuencia en la entidad financiera del Banco de Crédito del Perú, Puno 2024.				
P.E.2. ¿Cuál es el estado de seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024?	O.E.2. Identificar el estado de seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024.	H.E.2. No se tiene seguridad bancaria en la entidad financiera del Banco de Crédito del Perú, Puno 2024.				

Apéndice 2 Instrumento 1

ENCUESTA SOBRE LA IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA Y LA VULNERACIÓN DE LA SEGURIDAD BANCARIA

Instrucciones: El siguiente cuestionario tiene como objetivo recolectar información sobre la impunidad de la ciberdelincuencia financiera y la vulneración de la seguridad bancaria. Sus respuestas serán confidenciales y utilizadas únicamente para fines académicos.

Cuestionario:

ÍTEMS	VALORES	
	SI	NO
¿Está usted al tanto de los delitos cibernéticos financieros que afectan a los bancos?		
¿Conoce usted algún tipo específico de delito cibernético financiero (por ejemplo, phishing, malware, etc.)?		
¿Con qué frecuencia ha escuchado sobre ataques cibernéticos en el Banco de Crédito del Perú?		
¿Ha experimentado personalmente o conoce a alguien que haya sufrido un ataque cibernético relacionado con su cuenta bancaria en el último año?		
¿Cree que los ataques cibernéticos han afectado la seguridad de las cuentas bancarias en su banco?		
Si ha sido víctima de un ataque cibernético, ¿cómo afectó esto su cuenta bancaria?		
¿Cuál considera que ha sido el impacto financiero de los ataques cibernéticos en los clientes del Banco de Crédito del Perú?		
¿Cree que el impacto financiero de la ciberdelincuencia podría afectar su decisión de utilizar servicios bancarios en el futuro?		
¿Qué tan seguro se siente al realizar transacciones bancarias en línea?		

¿Confía en que el Banco de Crédito del Perú tiene medidas adecuadas para proteger sus transacciones en línea?		
¿Cómo calificaría las medidas de seguridad implementadas por su banco para proteger a los clientes de ciberdelincuencia?		
¿Está informado sobre las medidas de seguridad que su banco implementa para proteger sus datos personales y financieros?		
Si ha sido víctima de un ataque cibernético, ¿qué medidas tomó para reportar el incidente?		
¿Cuán efectivo considera que fue el procedimiento seguido por su banco tras un ataque cibernético?		
¿Está satisfecho con la respuesta de su banco después de un ataque cibernético?		
¿Considera que su banco proporciona suficiente apoyo y asesoramiento a los clientes que han sido víctimas de ciberdelincuencia?		

Gracias por su participación

Apéndice 4 Validez de Instrumento

FICHA DE VALIDACIÓN DEL INSTRUMENTO OPINIÓN DEL EXPERTO

I. DATOS GENERALES

1.1. Autor del instrumento: KATIA FIORELA APAZA FLORES

1.2. Validado por: Dr. JESUS MANUEL CRUZ CERVANTES

1.3. Título de la investigación:

VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024

1.4. Nombre del instrumento: CUESTIONARIO

II. ASPECTOS A EVALUAR

Nº	INDICADORES		VALORACIÓN																			
			DEFICIENTE				BAJO				REGULAR				BUENA				EXCELENTE			
			1	9	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
			5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1	CLARIDAD	Esta formado con lenguaje apropiado.																X				
2	OBJETIVIDAD	Está expresado en conductas observables.																X				
3	ACTUALIDAD	Está adecuado al avance de la ciencia.																X				
4	ORGANIZACIÓN	Existe una organización lógica.																X				
5	SUFICIENCIA	El número de ítems propuesto es suficiente para medir la variable.																X				
6	ADECUACIÓN	Está adecuado para valorar la variable de estudio.																X				
7	CONSISTENCIA	Está basado en aspectos teóricos y científicos.																X				
8	COHERENCIA	Existe coherencia entre el problema, objetivos e hipótesis.																X				
9	METODOLOGÍA	Responde al propósito de la investigación.																X				
10	PERTINENCIA	Es útil y adecuado para la investigación.																X				

III. **OPINIÓN DE APLICABILIDAD:** BUENA

IV. **PROMEDIO DE VALORACIÓN:** 80 %

V. **OBSERVACIONES:** NINGUNA

LUGAR Y FECHA: 08/09/25

FIRMA DEL EXPERTO
DNI 02419986

FICHA DE VALIDACIÓN DEL INSTRUMENTO OPINIÓN DEL EXPERTO

I. DATOS GENERALES

1.1. Autor del instrumento: KATIA FIORELA APAZA FLORES

1.2. Validado por: Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO

1.3. Título de la investigación:

VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024

1.4. Nombre del instrumento: CUESTIONARIO

II. ASPECTOS A EVALUAR

Nº	INDICADORES		VALORACIÓN																			
			DEFICIENTE				BAJO				REGULAR				BUENA				EXCELENTE			
			1	9	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
			5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1	CLARIDAD	Esta formado con lenguaje apropiado.																X				
2	OBJETIVIDAD	Está expresado en conductas observables.																X				
3	ACTUALIDAD	Está adecuado al avance de la ciencia.																X				
4	ORGANIZACIÓN	Existe una organización lógica.																X				
5	SUFICIENCIA	El número de ítems propuesto es suficiente para medir la variable.																X				
6	ADECUACIÓN	Está adecuado para valorar la variable de estudio.																X				
7	CONSISTENCIA	Está basado en aspectos teóricos y científicos.																X				
8	COHERENCIA	Existe coherencia entre el problema, objetivos e hipótesis.																X				
9	METODOLOGÍA	Responde al propósito de la investigación.																X				
10	PERTINENCIA	Es útil y adecuado para la investigación.																X				

III. **OPINIÓN DE APLICABILIDAD:** BUENA

IV. **PROMEDIO DE VALORACIÓN:** 80%

V. **OBSERVACIONES:** NINGUNA

LUGAR Y FECHA: 08/07/2025

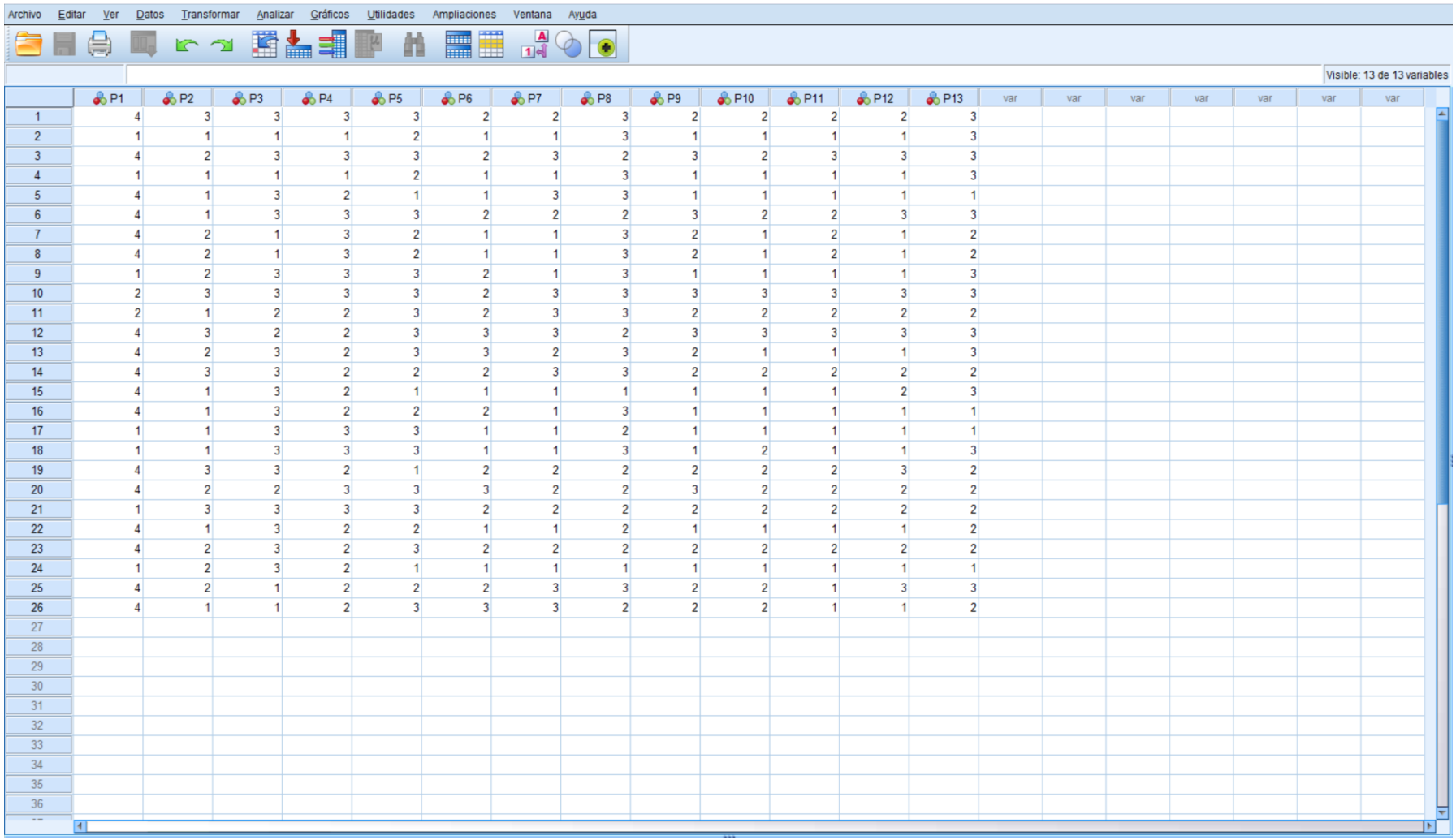
FIRMA DEL EXPERTO
Dr. Felix C. Ochatoma Paravicino
DNI 02436114

Apéndice 5 Matriz instrumental

V1: Ciberdelincuencia financiera			
Dimensiones	**Indicadores**	**Ítems**	**Valores**
Tipos de delitos cibernéticos	Conocimiento de los delitos cibernéticos financieros	¿Está usted al tanto de los delitos cibernéticos financieros que afectan a los bancos?	Si No
		¿Conoce usted algún tipo específico de delito cibernético financiero (por ejemplo, phishing, malware, etc.)?	Si No
	Frecuencia de ataques	¿Con qué frecuencia ha escuchado sobre ataques cibernéticos en el Banco de Crédito del Perú?	Si No
		¿Ha experimentado personalmente o conoce a alguien que haya sufrido un ataque cibernético relacionado con su cuenta bancaria en el último año?	Si No
Consecuencias de los ataques	Afectación de las cuentas bancarias	¿Cree que los ataques cibernéticos han afectado la seguridad de las cuentas bancarias en su banco?	Si No
		Si ha sido víctima de un ataque cibernético, ¿cómo afectó esto su cuenta bancaria?	Si No
	Percepción del impacto financiero	¿Cuál considera que ha sido el impacto financiero de los ataques cibernéticos en los clientes del Banco de Crédito del Perú?	Si No
		¿Cree que el impacto financiero de la ciberdelincuencia podría afectar su decisión de utilizar servicios bancarios en el futuro?	Si No
V2: Vulneración de la seguridad bancaria			
Dimensiones	**Indicadores**	**Ítems**	**Valores**
Confianza en la seguridad bancaria	Nivel de confianza en la seguridad de las transacciones bancarias	¿Qué tan seguro se siente al realizar transacciones bancarias en línea?	Si No
		¿Confía en que el Banco de Crédito del Perú tiene medidas adecuadas para proteger sus transacciones en línea?	
		¿Cómo calificaría las medidas de seguridad implementadas	Si No

	Percepción de las medidas de seguridad	por su banco para proteger a los clientes de ciberdelincuencia?	
		¿Está informado sobre las medidas de seguridad que su banco implementa para proteger sus datos personales y financieros?	Si No
Reacción ante un ataque cibernético	Procedimientos seguidos después de ser víctima de un ataque	Si ha sido víctima de un ataque cibernético, ¿qué medidas tomó para reportar el incidente?	Si No
		¿Cuán efectivo considera que fue el procedimiento seguido por su banco tras un ataque cibernético?	Si No
	Satisfacción con las acciones del banco ante un ataque	¿Está satisfecho con la respuesta de su banco después de un ataque cibernético?	Si No
		¿Considera que su banco proporciona suficiente apoyo y asesoramiento a los clientes que han sido víctimas de ciberdelincuencia?	Si No

Apéndice 6 Matriz de sistematización



Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

Visible: 13 de 13 variables

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	var	var	var	var	var	var	var
1	4	3	3	3	3	2	2	3	2	2	2	2	3							
2	1	1	1	1	2	1	1	3	1	1	1	1	3							
3	4	2	3	3	3	2	3	2	3	2	3	3	3							
4	1	1	1	1	2	1	1	3	1	1	1	1	3							
5	4	1	3	2	1	1	3	3	1	1	1	1	1							
6	4	1	3	3	3	2	2	2	3	2	2	3	3							
7	4	2	1	3	2	1	1	3	2	1	2	1	2							
8	4	2	1	3	2	1	1	3	2	1	2	1	2							
9	1	2	3	3	3	2	1	3	1	1	1	1	3							
10	2	3	3	3	3	2	3	3	3	3	3	3	3							
11	2	1	2	2	3	2	3	3	2	2	2	2	2							
12	4	3	2	2	3	3	3	2	3	3	3	3	3							
13	4	2	3	2	3	3	2	3	2	1	1	1	3							
14	4	3	3	2	2	2	3	3	2	2	2	2	2							
15	4	1	3	2	1	1	1	1	1	1	1	2	3							
16	4	1	3	2	2	2	1	3	1	1	1	1	1							
17	1	1	3	3	3	1	1	2	1	1	1	1	1							
18	1	1	3	3	3	1	1	3	1	2	1	1	3							
19	4	3	3	2	1	2	2	2	2	2	2	3	2							
20	4	2	2	3	3	3	2	2	3	2	2	2	2							
21	1	3	3	3	3	2	2	2	2	2	2	2	2							
22	4	1	3	2	2	1	1	2	1	1	1	1	2							
23	4	2	3	2	3	2	2	2	2	2	2	2	2							
24	1	2	3	2	1	1	1	1	1	1	1	1	1							
25	4	2	1	2	2	2	3	3	2	2	1	3	3							
26	4	1	1	2	3	3	3	2	2	2	1	1	2							
27																				
28																				
29																				
30																				
31																				
32																				
33																				
34																				
35																				
36																				

ANEXO 1
FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital [X] Fecha de entrega: 15/09/2025

1. Datos del autor (es):

Nombres y Apellidos: KATIA FIORELA APAZA FLORES
Dirección: Jr. DEZA 653
DNI/Carné de Extranjería/Pasaporte N°: 44609102
Teléfono: 933 812 015 email: katiafiorelaapazaflores@gmail.com
Nombres y Apellidos:
Dirección:
DNI/Carné de Extranjería/Pasaporte N°:
Teléfono: email:
Facultad y/o Escuela de Posgrado: CIENCIAS JURÍDICAS Y POLÍTICAS
Escuela Profesional o Mención: DERECHO
Título o Grado Académico a optar: ABOGADA
Asesor: Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO
Esta obra se encuentra dentro de las siguientes denominaciones:
Trabajo de Investigación [ ] Tesis [X] Trabajo de Suficiencia Profesional [ ] Trabajo Académico [ ]
Título: VULNERACIÓN DE LA SEGURIDAD BANCARIA E IMPUNIDAD DE LA CIBERDELINCUENCIA FINANCIERA, PUNO 2024

Palabras claves, (3 a 5 términos): Ciberdelincuencia, banco, impunidad, seguridad bancaria

¿Esta obra se desarrolló en la UANCV [1, 2]?
2

[1] Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entré otros relacionados.
[2] Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.

2. Referencia de tesis:

☐ Bachiller ☒ Titulo ☐ 2da Especialidad ☐ Maestría ☐ Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción Intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

☒ Sí, autorizo que se deposite inmediatamente.

☐ Sí, autorizo que se deposite a partir de la fecha (d/m/a):_____

☐ No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comérciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

☐ Sí autorizo

☒ No autorizo

Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción "internacional" o una adaptada a su jurisdicción, como para el caso peruano.

La opción "internacional" emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción "internacional" goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral**. Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

☒ Internacional

☐ Nacional

Línea de investigación: DERECHO PÚBLICO - P05

15 DE SETIEMBRE DEL 2025

Firma de Autor | huella digital | Fecha