INSTITUTO DE GOBIERNO Y DE GESTIÓN PÚBLICA
UNIDAD DE POSGRADO

LAS MEDIDAS DE SEGURIDAD EN LAS OPERACIONES BANCARIAS POR INTERNET SEGÚN LOS ORGANOS RESOLUTIVOS DE PROCEDIMIENTOS SUMARÍSIMOS DEL INDECOPI DE ICA, AREQUIPA Y TACNA 2021

PRESENTADO POR
MARITZA ELIZABETH OCHOA QUISPE

ASESOR
RENAN QUISPE LLANOS

TRABAJO DE INVESTIGACIÓN
PARA OPTAR EL GRADO ACADÉMICO DE MAESTRA EN GESTIÓN PÚBLICA

LÍNEA DE INVESTIGACIÓN
SISTEMAS ADMINISTRATIVOS DEL ESTADO

LIMA – PERÚ
2021

INSTITUTO DE GOBIERNO Y DE GESTIÓN PÚBLICA

SECCIÓN DE POSGRADO

“LAS MEDIDAS DE SEGURIDAD EN LAS OPERACIONES BANCARIAS POR INTERNET SEGÚN LOS ORGANOS RESOLUTIVOS DE PROCEDIMIENTOS SUMARÍSIMOS DEL INDECOPI DE ICA, AREQUIPA Y TACNA 2021”

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO

DE MAESTRA EN GESTIÓN PÚBLICA

PRESENTADO POR:

MARITZA ELIZABETH OCHOA QUISPE

ASESOR:

Dr. RENAN QUISPE LLANOS

LÍNEA DE INVESTIGACIÓN:

SISTEMAS ADMINISTRATIVOS DEL ESTADO

LIMA, PERÚ

2021

DEDICATORIA

Dedico este trabajo de investigación a mis queridos padres, en especial a mi difunto papá quien hace un mes partió a la eternidad a puertas de alcanzar este nuevo logro; por ser mi fuente de inspiración, motivación y confianza. Gracias por todo su apoyo para alcanzar mis metas trazadas y creer en mí.

Maritza Elizabeth Ochoa Quispe

AGRADECIMIENTO

Agradezco al asesor del Trabajo de Investigación, Dr. Renán Quispe Llanos, quien me brindó las pautas necesarias para el desarrollo del trabajo y permitió lograr su culminación con éxito.

Maritza Elizabeth Ochoa Quispe

ÍNDICE DE CONTENIDO

PORTADA i
DEDICATORIA ii
AGRADECIMIENTO iii
INDICE DE CONTENIDO iv
INDICE DE TABLAS vi
RESUMEN viii
ABSTRACT x
INTRODUCCION 1
Descripción de la situación problemática 1
Formulación del Problema 8
Objetivos de la Investigación 8
Justificación de la investigación 9
Limitaciones del estudio 11
CAPÍTULO I: MARCO TEÓRICO 12
1.1. Antecedentes de la investigación 12
1.1.1. Antecedentes Internacionales 12
1.1.2. Antecedentes nacionales 13
1.2. Bases teóricas 15
1.2.1. Definición de la tarjeta de débito 15
1.2.2. Definición de tarjeta de crédito 16
1.2.3. Sistema Bancario 16
1.2.4. Protocolos de seguridad integrados en tarjetas de crédito y débito 16
1.2.5. Medidas de seguridad respecto a la realizacion de operaciones en las tarjetas de crédito y débito 20
1.2.6. Educación Financiera 194
1.2.7. Reglamento de tarjetas de crédito y débito de la SBS N° 6523-2013 24
1.3. Definición de términos básicos 26
1.3.1. Servicio De Atención al Ciudadano 26
1.3.2. Órganos Resolutivos de Procedimientos Sumarísimos 26
1.3.3. Comisiones de Protección al Consumidor 27
1.3.4. Sala Especializada en Protección Al Consumidor 27
1.3.5. Comportamiento habitual de consumo del usuario 27
1.3.6. Tarjeta de crédito 28
1.3.7. Tarjeta de débito 28
1.3.8. Fraude electronico 28
1.3.9. Operaciones no reconocidas 30
1.3.10. Información sobre la posición de una de las entidades bancarias que forma

parte de la investigación sobre la adopción de medidas de seguridad frente a operaciones no reconocidas por internet 31
CAPÍTULO II: OPERACIONALIZACIÓN DE VARIABLES 37
2.1. Variable Independiente: Medidas de seguridad 37
2.2. Variable Dependiente: Operaciones por internet 37
2.3. Dimensiones 37
2.4. Matriz de operacionalización de variables 45
CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN 45
3.1. Diseño metodológico 51
3.2. Diseño muestral 51
3.2.1. Población 52
3.2.2. Muestra 53
3.3. Técnicas de recolección de datos 56
3.4. Técnicas de gestión y estadísticas para el procesamiento de la información 57
3.5. Aspectos éticos 58
CAPÍTULO IV: RESULTADOS Y PROPUESTA DE VALOR 59
4.1. RESULTADOS 59
PROPUESTA DE VALOR 104
CAPITULO V: DISCUSIÓN 110
CONCLUSIONES 114
RECOMENDACIONES 116
FUENTES DE INFORMACIÓN 117
ANEXOS 123

INDICE DE TABLAS

Tabla 1. Ranking de los diez (10) proveedores sancionados (SISTEMA FINANCIERO BANCARIO) del 2021 5

Tabla 2. Denuncias ante el Órgano Resolutivo de Procedimientos Sumarísimos de la Oficina Regional del INDECOPI de Ica en el 2021 6

Tabla 3. Denuncias registradas por entidad en el 2021 7

Tabla 4. Matriz de operacionalización de variables 45

Tabla N° 5: Nivel de seguridad en el chip de las tarjetas de débito y crédito. 59

Tabla N° 6: Niveles de eficiencia respecto de los procedimientos criptográficos sobre datos críticos 60

Tabla N° 7: Niveles de eficiencia en usar métodos autentificación de datos 61

Tabla N° 8: Niveles de eficiencia respecto de las instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea 62

Tabla N° 9: Niveles de eficiencia sobre la entrega de tarjeta a titular 64

Tabla N° 10: Nivel de eficiencia respecto al cambio de primera clave o número secreto de la tarjeta 65

Tabla N° 11: Nivel de eficiencia respecto al servicio de notificaciones mediante mensajes de texto, a un correo electrónico y/o un teléfono móvil, entre otros mecanismos. 66

Tabla N° 12: Niveles de eficiencia respecto de comunicar a la empresa que realizarán operaciones con su tarjeta desde el extranjero 67

Tabla N° 13: Niveles de eficiencia de los sistemas de monitoreo de operaciones que detectan operaciones que no corresponden al comportamiento habitual de consumo del usuario 68

Tabla N° 14: Nivel de eficiencia respecto de la identificación de patrones de fraude 70

Tabla N° 16: Niveles de eficiencia en la presentación de un documento oficial de identidad. 72

Tabla N° 17: Niveles de eficiencia de configuración de cortafuegos o firewalls, enrutadores y equipos similares 73

Tabla N° 18: Niveles de eficiencia del software y programas antivirus en computadores y servidores 74

Tabla N° 19: Niveles de eficiencia de los sistemas informáticos y aplicaciones seguras para las operaciones por internet 75

Tabla N° 20: Niveles de eficiencia de las políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados provistos por los proveedores de servicios de tecnología 77

Tabla N° 21: Niveles de eficiencia de las políticas que restrinjan el acceso a los datos de los usuarios solo al personal autorizado, reduciéndolo al estrictamente necesario. 78

Tabla N° 22: Niveles de eficiencia de las políticas de asignación de un identificador único a cada persona que acceda a través de software a los datos de los usuarios 80

Tabla N° 23: Niveles de eficiencia de los controles de acceso físico para proteger los datos de los usuarios. 81

Tabla N° 24: Niveles de eficiencia del registro y monitoreo todos los accesos a los recursos de red y a los datos de los usuarios 82

Tabla N° 26: Grado de eficiencia del plan de respuesta a eventos de violación de seguridad. 84

Tabla N° 27: Niveles de eficiencia de los procedimientos de aceptación de las operaciones, incluyendo entre otros la verificación de la validez de la tarjeta, la identidad del usuario, y la firma en caso de ser aplicable. 85

Tabla N° 28: Grado de eficiencia de no guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta. 86

Tabla N° 29: Niveles de conocimiento que pueden realizar operaciones en internet con su tarjeta de crédito y/o débito 87

Tabla N° 30: Conocimiento de haber realizado alguna vez operaciones por internet 88

Tabla N° 31: Tipos de operaciones que han realizado en el último año a través de la Banca Móvil o mediante la Banca por Internet. 89

Tabla N° 32: Aplicaciones que han utilizado para realizar operaciones en internet 90

Tabla N° 33: Problema con el uso fraudulento de su tarjeta de crédito y/o débito en el último año. 91

Tabla N° 34: Pedido de identificación del tarjeta habiente para realizar una operación con tarjeta de crédito. 92

Tabla N° 35: Experiencia al realizar operaciones por internet 93

Tabla N° 36: Grado de interés de efectuar operaciones por internet 94

Tabla N° 37: Ventajas sobre las operaciones por internet 95

Tabla 39: Relación entre las medidas de seguridad incorporadas en las tarjetas de débito y crédito, y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna 98

Tabla 40: Relación entre las medidas de seguridad respecto a los usuarios y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna 100

Tabla 41: Relación entre las medidas de seguridad respecto al monitoreo y realización de operaciones, y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna 101

Tabla 42: Relación entre las variables: medidas de seguridad respecto al uso de tarjetas de débito y crédito, y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna 102

RESUMEN

Durante el año 2021 se presentaron diversas denuncias en los Órganos Resolutivos de Procedimientos Sumarísimos del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual de Ica, Arequipa y Tacna (en adelante, Los ORPS del INDECOPI de Ica, Arequipa y Tacna) lo que motivó la investigación sobre la correlación existente entre las medidas de seguridad y las operaciones por internet.

La elección del presente trabajo de investigación se ha desarrollado buscando tesis, noticias, resoluciones expedidas por el Indecopi colgadas en su repositorio institucional de acceso público que avalan el tema de investigación a través de los cuales se ha encontrado antecedentes que ha llegado a concluir que las medidas de seguridad implementadas por las entidades financieras y bancarias en cumplimiento a la Resolución SBS 6523-2023 modificada por la Resolución SBS 5570-20219 (Reglamento de Tarjetas de Crédito y Débito) no vienen siendo aplicadas de manera idónea por estos últimos con mayor incidencia en las operaciones por internet generando afectación en la economía del consumidor al efectuarse fraude electrónico con tarjetas de crédito y débito.

Se ha propuesto como objetivo demostrar de qué manera las medidas de seguridad están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna del periodo 2021.

En el presente trabajo de investigación se ha tomado como instrumentos de la investigación encuestas directas aplicadas a los servidores públicos de las oficinas regionales del INDECOPI de Ica, Arequipa y Tacna y asimismo a los Usuarios que presentaron denuncias sobre el tema de investigación ante los

mencionados órganos resolutivos determinándose que pese a que existe una regulación por parte de la Superintendencia de Banca, Seguros y AFP sobre las medidas de seguridad que deben de implementar las entidades financieras y bancarias; no obstante a la fecha no se ha regulado cómo es que estos últimos deben de aplicar estas medidas, ocasionando que cada entidad si bien tiene implementado sus medidas de seguridad, las apliquen de manera indistinta bajo su propio criterio no existe uniformización de su aplicación respecto al monitoreo de las operaciones, hecho que se ve reflejado en el análisis de las resoluciones finales emitidas por los Órganos Resolutivos a nivel nacional del INDECOPI en los que forma parte los OPS Ica, Arequipa y Tacna sancionándolos demostrándose que las entidades financieras y bancarias no ofrecen un servicio idóneo al consumidor.

Asimismo se ha demostrado que también se incide como factor de incumplimiento de las medidad de seguridad la falta de educación financiera.

Las transacciones no reconocidas han ido en aumento desde el año 2021 hasta hoy, lo que generó que se solicite al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (En adelante, INDECOPI) estadísticas de denuncias por operaciones no reconocidas. Los datos arrojados indican que las entidades financieras no actúan con rapidez ni eficacia en la detección temprana de transacciones anómalas con tarjetas de crédito y débito en relación a su deber de monitoreo.

ABSTRACT

During the year 2021, several complaints were filed in the Resolving Bodies of Summary Proceedings of the National Institute for the Defense of Competition and Protection of Intellectual Property of Ica, Arequipa and Tacna (hereinafter ORPS of INDECOPI of Ica, Arequipa and Tacna) that motivated the research on the existing correlation between security measures and operations on the Internet.

The choice of the present research work has been developed through the search of theses, news, resolutions issued by Indecopi published in its institutional repository of public access that support the research topic through which background information has been found that has allowed concluding that the security measures implemented by financial and banking entities in compliance with Resolution SBS 6523- 2023, modified by Resolution SBS 6523- 2023, modified by Resolution SBS 6523- 2023, modified by Resolution SBS 6523- 2023. 2023 modified by SBS Resolution 5570-20219 (Credit and Debit Card Regulations) are not being adequately applied by the latter, with greater incidence in Internet operations, generating affectation in the consumer's economy due to electronic fraud with credit and debit cards.

The objective is to demonstrate how security measures are related to Internet banking operations according to the ORPS of INDECOPI in Ica, Arequipa and Tacna for the period 2021.

In this research work, direct surveys were carried out with public servants from INDECOPI's regional offices in Ica, Arequipa and Tacna, as well as with users who filed complaints on the subject of the investigation before the aforementioned regulatory bodies, determining that although there is a regulation by the

Superintendence of Banking, Insurance and AFP on the security measures that financial and banking entities must implement, to date there is no regulation on how the latter must apply these measures; However, to date there is no regulation on how the latter should apply these measures, causing each entity, although it has implemented its security measures, to apply them indistinctly under its own criteria and there is no uniformity in their application with respect to the monitoring of operations, This is reflected in the analysis of the final resolutions issued by INDECOPI's national resolution bodies, including the Ica, Arequipa and Tacna OPSs, which sanctioned them, demonstrating that financial and banking entities do not offer an adequate service to consumers.

It has also been demonstrated that the lack of financial education is also a factor of non-compliance with security measures.

Unrecognized transactions have been increasing from 2021 to date, which led to a request to the National Institute for the Defense of Competition and Protection of Intellectual Property (hereinafter INDECOPI) for statistics on complaints of unrecognized transactions. The data obtained indicate that financial entities do not act quickly or effectively in the early detection of anomalous transactions with credit and debit cards in relation to their duty of monitoring.

Similarity Report

PAPER
VERSION ULTIMA TESIS MARITZA ELIZA BETH OCHOAQUISPE RESUMEN.docx

AUTHO
MARITZA ELIZABETH OCHOA QUISPE

WORD COUNT
11491 Words

CHARACTER COUNT
62065 Characters

PAGE COUNT
80 Pages

FILE SIZE
1.1MB

SUBMISSION DATE
May 8, 2023 10:25 AMGMT-5

REPORT DATE
May 8, 2023 10:30 AM GMT-5

18% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 16% Internet database
- 6% Publications database
- Crossref database
- Crossref Posted Contentdatabase
- 13% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 8 words)

Summary

INTRODUCCION

Descripción de la situación problemática

En tiempos actuales, los usuarios de las instituciones financieras y bancarias están recurriendo a otras alternativas de realizar operaciones financieras desfasando las físicas por las virtuales debido a la expansión de la economía peruana. El crecimiento ha provocado el lanzamiento de una serie de categorías de productos financieros, como tarjetas de débito y crédito. Estas alternativas facilitan transacciones financieras por montos elevados que minimiza la exposición a ser victima de la delincuencia callejera.

El mayor número de transacciones a través de canales digítales o electrónicos, así como el creciente uso de las tarjetas para adquirir bienes y servicios en comercios online, hacen necesario un refuerzo de los mecanismos de seguridad implementados por la SBS en cautela de los derechos de los tarjetahabientes.

El Reglamento de Tarjetas de Crédito y Débito (Resolución S.B.S 6523-2013) y con su modificatoria la Resolución N° 5570-2019 establece que a fin de evitar el fraude electrónico, las entidades del sistema bancario deben adoptar medidas de seguridad definidas en su artículo 17°; esto en concordancia con la calidad e idoneidad del servicio, es decir que las entidades financieras y bancarias por ofrecer servicios de naturaleza riesgosa debe tener las suficientes medidas de seguridad para que ante cualquier contingencia o fraude electrónico se proteja el patrimonio del consumidor ya que es la parte vulnerable.

El propósito de este trabajo de investigación a través de los instrumentos de la investigación encuestas directas aplicadas a los servidores públicos de las oficinas regionales del INDECOPI de Ica, Arequipa y Tacna y asimismo a los Usuarios que presentaron denuncias sobre el tema de investigación ante los mencionados órganos resolutivos (ello debido a que se analiza la afectación que les causa las entidades financieras y bancarias al efectuarse operaciones fraudulentas electrónicamente con el uso de sus tarjetas de crédito y débito) determinándose que pese a que existe una regulación por parte de la Superintendencia de Banca, Seguros y AFP sobre las medidas de seguridad que deben de implementar las entidades financieras y bancarias; no obstante a la fecha no se ha regulado cómo es que estos últimos deben de aplicar estas medidas, ocasionando que cada entidad si bien tiene implementado sus medidas de seguridad, las apliquen de manera indistinta bajo su propio criterio no existe uniformización de su aplicación respecto al monitoreo de las operaciones, hecho que se ve reflejado en el análisis de las resoluciones finales emitidas por los Órganos Resolutivos a nivel nacional del INDECOPI en los que forma parte los OPS Ica, Arequipa y Tacna sancionándolos demostrándose que las entidades financieras y bancarias no ofrecen un servicio idóneo al consumidor.

Asimismo se ha demostrado que también se incide como factor de incumplimiento de las medidad de seguridad la falta de educación financiera.

En Perú, dos de las instituciones estatales que regulan, supervisan y sancionan a los bancos y otras entidades financieras —cajas municipales, cajas rurales y financieras, entre otras— son el Indecopi y la Superintendencia de Banca y Seguros del Perú (SBS). Mientras que la primera sanciona a las empresas del

sector financiero por afectaciones a los derechos del consumidor, la segunda vigila la regulación y sanciona a los bancos el incumplir las normas que emitieron en el sector financiero (no se aplica para casos particulares, usuarios que denuncien, ello lo remite al INDECOPI al no ser su competencia).

Indecopi es la autoridad competente para resolver controversias de protección al consumidor del sector financiero, mientras que la SBS vela por la adecuada gestión de conducta de mercado de las entidades del sector financiero.

Las competencias del INDECOPI y de la SBS son distintas toda vez que el primero de ellos protege al consumidor en tanto este es titular de un interés particular de protección de sus derechos personales por ejemplo en materia financiera, mientras que la SBS procura la estabilidad del sistema financiero en su conjunto, es decir, vela por un interés general y público. La competencia de la SBS es ver que “el avión no se caiga”, la competencia del INDECOPI es velar porque cada pasajero esté bien atendido.

El marco jurídico para la protección general ante operaciones no reconocidas via internet, no solo se haya en el Reglamento de Tarjetas de Crédito y Débito de la SBS, sino también en el Codigo de Protección y Defensa del Consumidor, el cual ha establecido normas de protección de los consumidores en servicios financieros.

En base a ello, el INDECOPI a través de la Sala Especializada en Protección al Consumidor ha brindado criterios respecto a la responsabilidad administrativa del proveedor en el caso de medidas de seguridad ante riesgos inherentes a las tarjetas de crédito y débitos, ello mediante el reconocimiento de operaciones inusuales y las acciones que debió tomar el consumidor y el proveedor.

Debido a ello, INDECOPI tiene la facultad de realizar investigaciones, de implementar las medidas correctivas correspondientes y de imponer las sanciones administrativas necesarias al emitir algún pronunciamiento sobre el procedimiento llevado a cabo.

Es necesario precisar que la reducción de riesgos en las tarjetas de crédito requiere de la adopción de medidas de seguridad eficientes que se adacten a la evolución tecnológica del país, en tanto las nuevas formas de tecnología o su nuevo uso permiten nuevas formas de fraude en los servicios financieros. En base a ello, se requiere que las medidas de seguridad reduzcan los riesgos inherentes a las tarjetas de crédito y débito y se genere una forma más eficaz de protección al consumidor, por lo tanto, ante la ausencia o deficiencia de estas medidas, se atribuye responsabilidad administrativa a la entidad bancaria.

Es necesario que se tomen en cuenta la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702, la cual permite a las empresas del sistema financiero a expedir y administrar tarjetas de crédito, la Resolución SBS Nº 6523-2013 y modificatorias, la cual reglamenta el producto de tarjetas de crédito y debido, con la finalidad de reducir algún uso fraudulento, y la Resolución S.B.S. 3274-2017 que trata sobre la gestión de conducta de mercado en el sistema financiero.

El año pasado, la Asociación de Bancos del Perú reveló que el robo digital representó el 38% de todos los casos relacionados con el robo de tarjetas de crédito y débito. Previo a septiembre de 2020, más de 6 millones de soles desaparecieron por estafas en línea, según informó la Policía Nacional del Perú. Estas circunstancias se derivan de los protocolos ante la pandemia de COVID-19

instituidos por el gobierno y la preocupación por la salud pública, que elevó la compra de bienes y pagos de servicios en línea y el consecuente aumento de actividades fraudulentas. En particular, la División de Investigación de Delitos de Alta Tecnología se encargó de investigar estos casos. (pág. 1)

Como resultado, los consumidores han formulado denuncias, dando como resultado un ranking de los diez (10) proveedores más sancionados del sistema financiero bancario en el 2021.

En 2021, los proveedores financieros sancionados se clasificaron después de que los clientes presentaran denuncias administrativas. Esta clasificación fue consecuencia de los reclamos de los clientes dentro del sistema financiero.

Tabla 1. Ranking de los diez (10) proveedores sancionados (SISTEMA FINANCIERO BANCARIO) del 2021

Nro.	Razón social	Nombre comercial	Total de sanciones	Monto UIT
1	BANCO DE CRÉDITO DEL PERU S.A	BANCO DE CREDITO DEL PERU S.A.	351	215.22
2	BANCO BBVA PERÚ S.A	BBVA	323	314.58
3	BANCO INTERNACIONAL DEL PERÚ S.A.A.- INTERBANK	INTERBANK	313	347.42
4	BANCO RIPLEY PERU S.A	BANCO RIPLEY	218	111.01
5	FINANCIERA OH! S.A O FINANCIERA OH S.A.	FINANCIERA OH! S.A O FINANCIERA OH S.A.	194	92.07
6	SCOTIABANK PERU S.A.A.		183	152.38
7	BANCO DE LA NACIÓN	BANCO DE LA NACION	90	101.58
8	BANCO FALABELLA PERU S.A.	BANCO FALABELLA	90	20.63
9	BANCO INTERAMERICANO DE FINANZAS S.A.	BIF	89	41.18
10	CAJA RURAL DE AHORRO Y CRÉDITO CENCOSUD SCOTIA PERU SA.	BANCO CENCOSUD SCOTIA (...)	81	33.79

Fuente: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

La clasificación de Registro de Infracciones y Sanciones se basa en el número total de sanciones reveladas para el período anual que comienza el 1 de enero de 2021 y finaliza el 31 de diciembre de 2021. Asimismo, se debe recalcar que la información corresponde al total de sanciones informadas en las decisiones del órgano resolutor y este es el número absoluto de sanciones registradas y no las presenta proporcionalmente al volumen de actividad o transacciones de cada proveedor. Cabe precisar que sólo se está haciendo mención a los diez (10) proveedores más sancionados que figura en mira a quien le compras del INDECOPI consultado el 16 de junio de 2022.

Las sanciones incluyen multas y amonestaciones. 2/ UIT: Unidades Impositivas Tributarias. En caso de tener una sanción igual a cero (0.00 UIT) esta se refiere a una amonestación.

Según la estadística del INDECOPI, en el Órgano Resolutivo de Procedimientos Sumarísimos de Ica, en el 2021 se registraron un total de 319 denuncias, de las cuales 196 denuncias fueron del rubro financiero y bancario, y una cifra de 107 denuncias por operaciones no reconocidas vía internet y/o aplicativos móviles.

Tabla 2. Denuncias ante el Órgano Resolutivo de Procedimientos Sumarísimos de la Oficina Regional del INDECOPI de Ica en el 2021

TOTAL, DE DENUNCIAS ÓRGANO RESOLUTIVO DE PROCEDIMIENTOS SUMARÍSIMOS DE ICA EN EL 2021	TOTAL, DE DENUNCIAS FINANCIERO BANCARIO EN EL 2021	TOTAL, DE DENUNCIAS POR OPERACIONES NO RECONOCIDAS VIA INTERNET 2021
319	196	107

Fuente: Órgano Resolutivo de Procedimientos Sumarísimos del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual de Ica.

El ORPS de Ica en el año 2021 registró 107 denuncias por transacciones no reconocidas - comercio electrónico (internet, aplicaciones móviles, etc.) en el sistema bancario y financiero ante los siguientes proveedores:

Tabla 3. Denuncias registradas por entidad en el 2021

DENUNCIADO	TIPO / NRO. DOCUMENTO	N° DENUNCIAS
BANCO FALABELLA PERU S.A	RUC : 20330401991	31
BANCO INTERNACIONAL DEL PERU S.A.A.-INTERBANK	RUC : 20100053455	16
BANCO DE LA NACIÓN	RUC : 20100030595	13
BANCO BBVA PERU S.A.	RUC : 20100130204	12
BANCO RIPLEY PERU S.A.	RUC : 20259702411	10
FINANCIERA OH! S.A O FINANCIERA OH S.A	RUC : 20522291201	07
SCOTIABANK PERU S.A. A	RUC : 20100043140	06
BANCO DE CREDITO DEL PERU S.A.	RUC : 20100047218	06
CREDISCOTIA FINANCIERA S.A.	RUC : 20255993225	03
CAJA RURAL DE AHORRO Y CRÉDITO CENCOSUD SCOTIA PERÚ S.A.	RUC : 20543166660	01
BANCO INTERAMERICANO DE FINANZAS S.A.	RUC : 20101036813	01
ALFIN BANCO S.A.	RUC : 20517476405	01

Fuente: Órgano Resolutivo de Procedimientos Sumarísimos del INDECOPI de Ica.

Formulación del Problema

Problema General

- ¿De qué manera las medidas de seguridad están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021?

Problemas Específicos

- ¿De qué manera las medidas de seguridad incorporadas en las tarjetas están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021?
- ¿De qué manera las medidas de seguridad respecto a los usuarios están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021?
- ¿De qué manera las medidas de seguridad respecto al monitoreo y realización de operaciones están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021?

Objetivos de la Investigación

Objetivo General

- Determinar de qué manera las medidas de seguridad están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021

Objetivos Específicos

- Determinar de qué manera las medidas de seguridad incorporadas en las tarjetas están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021

- Determinar de qué manera las medidas de seguridad respecto a los usuarios están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021.

- Determinar de qué manera las medidas de seguridad respecto al monitoreo y realización de operaciones están relacionadas con las operaciones bancarias por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021.

Justificación de la investigación

Importancia de la investigación

La investigación es imprescindible para adquirir nuevos conocimientos y hacer avanzar a la sociedad. Sin él, el progreso se detendría en seco. Todo avance científico o tecnológico proviene de la investigación. Las ideas se prueban y refinan para garantizar su eficacia y relevancia. Incluso en la vida diaria, la investigación se utiliza en la toma de decisiones, como elegir un producto en función de las reseñas o investigar un destino de viaje antes de reservar un viaje.

Para transformar el mundo para mejor, la presente investigación es importante porque aborda un tema sobre el cual no existen muchos estudios

realizados en el Perú, razón por la cual se ha escogido algunas tesis que tengan mayor relación con el tema de investigación.

El aumento de los ataques a la seguridad del sistema financiero de los clientes, específicamente las vulnerabilidades que afectan a los usuarios, las redes y el dominio web de los proveedores, y la falta de regulación y uniformidad de las medidad de seguridad de las entidades financieras referido a como debe de aplicarse estas medidas de seguridad, lo cual beneficiará a los consumidores reforzando la protección de sus intereses económicos en materia de servicios financieros.

Declarada por el gobierno, la emergencia sanitaria y la emergencia nacional han provocado que las personas realicen transacciones en línea con mayor frecuencia. A pesar de que esta es la norma hoy en día, el sistema financiero ha luchado para abordar los riesgos y las transacciones no autorizadas que conlleva.

Se debe crear propuestas de valor a través de esta investigación para generar una mayor confianza en los tarjetahabientes en el cumplimiento del deber de idoneidad de la entidad financiera referido a la adopción de medidas de seguridad frente a la realización de operaciones no reconocidas via internet con las tarjetas de crédito y débito que les expiden.

Viabilidad de la investigación

Para la investigación en cuestión, se requieren herramientas esenciales para el avance. Se efectuara encuestas directas anónimas a los servidores públicos de las Oficinas Regionales objeto de investigación y a su vez al público usuario, solicitando autorización a los jefes de las áreas investigadas para su aplicación.

Todos los gastos de investigación serán financiados por el investigador. Por último, se utilizará para el análisis una compilación de literatura perteneciente a la línea de investigación específica.

Limitaciones del estudio

En el contexto de la pandemia y emergencia sanitaria, poca investigación sobre el tema elegido.

CAPÍTULO I: MARCO TEÓRICO

1.1. Antecedentes de la investigación

1.1.1. Antecedentes Internacionales

Guarnizo & Segura (2018) señalan lo siguiente:

> Las entidades financieras tienen la responsabilidad por un fraude electrónico, debido a que su simple actividad exige que no solamente se deban tener mecanismos de control y seguridad, sino que también se debe responder de todas las amenazas y vulneraciones que se pueden llegar a presentar con los usuarios y sus respectivas cuentas. Es la entidad financiera quien debe ser responsable por la función de las actividades que realiza y no excusarse que por no utilizar las medidas de seguridad disminuye las obligaciones y responsabilidades frente a los usuarios. (págs. 99-126)

Para mantener una reputación positiva con sus clientes, Molano & Correa (2016) en la tesis “Predicción del fraude con tarjetas para una entidad financiera a través del modelo Arimax”, de la Universidad Los Libertadores- Sede Bogotá sugieren que las instituciones bancarias reduzcan los casos de fraude en Internet mediante la implementación de medidas de protección. (pág. 9).

Paz (2018) en el artículo científico “La culpa del consumidor en la responsabilidad financiera y proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones

Jurisdiccionales de la Superintendencia Financiera de Colombia", publicado en la Revista de Derecho Privado de la Universidad Externado de Colombia señala "que las entidades bancarias deben de tener especial cuidado en ofrecer a los consumidores servicios y productos de calidad. En ese sentido, se deben tomar acciones, a fin de evitar fraudes electrónicos. Si la entidad bancaria no cumple con las medidas para prevenir fraudes electrónicos se hallaría su responsabilidad" (págs. 261-289).

1.1.2. Antecedentes nacionales

Meza (2012) en la tesis para optar el título de abogado de la Pontificia Universidad Católica del Perú "El estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación", concluye que con las tarjetas tanto el Banco como los del establecimiento afiliado deberán cumplir con la idoneidad del servicio ante el usuario.

Mora (2020) profundizó en la toma de decisiones de la Sala Especializada en Protección al Consumidor del INDECOPI sobre las actividades de tarjetas de crédito y débito que pasaron desapercibidas en su análisis. También reflexionó sobre los protocolos de seguimiento que deben establecer las entidades financieras. El objetivo de su investigación fue conocer las reglas que debe aplicar la autoridad resolutiva del INDECOPI al momento de solicitar la devolución de fondos por alguna actividad irregular imputada a una tarjeta. Además, el artículo presenta recomendaciones destinadas a mejorar la gestión actual de transacciones con tarjetas de crédito y débito no reconocidas. (pág. 2)

Al observar las cifras de solicitudes y reclamos sobre transacciones no reconocidas que se tramitan en el INDECOPI, Balcazar (2017) realizó una investigación para determinar si ha habido un aumento en este tipo de operaciones desde 2014 hasta la actualidad. Reconocer una actividad inusual en las operaciones con tarjetas de crédito y débito no fue algo que las instituciones financieras investigaran fácilmente, como descubrió el autor durante su propia investigación. (págs. 4, 5)

En una investigación realizada por Linares (2020), el foco estuvo en las instituciones bancarias de la zona de Libertad para asegurar que estén cumpliendo adecuadamente con sus responsabilidades en lo que se refiere a prevenir el fraude electrónico a través de tarjetas de crédito y tarjetas de debito. A través de un examen minucioso que involucró 15 decisiones relevantes a transacciones no reconocidas a través de los Órganos Resolutivos de Procedimientos Sumarísimos del INDECOPI, una evaluación exhaustiva de las regulaciones globales, así como una encuesta de comentarios de los clientes, frente al fraude electrónico con tarjetas de crédito y débito, se ha dado a conocer que los bancos involucrados no cumplen con su deber de idoneidad. (pág. 7).

Al analizar los sistemas de monitoreo y alerta, Silvestre (2021) estudió el protocolo de seguridad de las instituciones financieras relacionado con las tarjetas de crédito y débito, con un enfoque de la actividad inusual. señalo que estos sistemas son responsabilidad del proveedor y fueron analizados para determinar su efectividad. Utilizando como guía los criterios establecidos por la Sala Especializada de Protección al

Consumidor, Silvestre recomendó medidas de seguridad para garantizar la seguridad de las transacciones con tarjetas. Los resultados de la investigación arrojan luz sobre la implementación de las medidas de seguridad. (pág. 3)

Al realizar una investigación en 2019, Cusacani y Ttito buscaron descubrir el vínculo entre la utilización de tarjetas de crédito y débito y la educación financiera. Los clientes de Banco Continental - Agencia Miraflores constituyeron el foco de su estudio, que finalmente expuso la esencialidad de la cultura financiera en el proceso de toma de decisiones en torno al uso de la tarjeta. (pág. 4)

1.2. Bases teóricas

1.2.1. Definición de la tarjeta de débito

La posibilidad de retirar y depositar efectivo en cajeros automáticos, así como utilizar fondos de una cuenta de ahorros vinculada para realizar compras en terminales de venta, son algunas de las características de la tarjeta de débito plástica con banda magnética, como lo señala Escoto (2007) (pág. 108).

“El uso de los fondos depositados en una cuenta (corriente o de ahorro) asociada a la misma, está permitido por la tarjeta de débito”, así describen Flores, Pilco y Haro (2015) esta forma de pago (pág. 1).

1.2.2. Definición de tarjeta de crédito

Flores Pilco y Haro (2015) definen las tarjetas de crédito como piezas plásticas rectangulares que permiten realizar compras sin efectivo, en donde el titular de la tarjeta puede optar por pagar al banco en un solo pago o en cuotas, según su conveniencia, luego de recibir el estado de cuenta. (pág. 2)

Según la definición de Flores Pilco y Haro de 2015, el proceso de compra sin efectivo se puede realizar a través de piezas plásticas rectangulares conocidas como tarjetas de crédito. El tarjetahabiente entonces tiene la opción de pagarle al banco en un pago único o en cuotas, según su preferencia, lo que ocurre después de que se recibe el estado de cuenta. (pág. 188)

1.2.3. Sistema Bancario

Según la “Superintendencia de Banca y Seguros y AFP” (SBS) en su guía “Programa finanzas en el cole” en el año 2017, señala que dicho sistema es aquel cuyo rubro de negocio es captar dinero del público en forma de depósito u otra modalidad contractual, y ofrecen créditos a las personas que lo necesitan en diferentes modalidades.

Asimismo, establece dos modalidades en las que se divide el sistema bancario siendo:

1.2.3.1 No Bancario

No son consideradas como Bancos, pero captan y canalizan los recursos; dentro de esta clasificación se encuentran:

1.2.3.1.1 Empresas Financieras

Aquellas que captan los recursos del público y facilitan la colocación de emisiones de valores, utilizando valores mobiliarios y brindan asesoría financiera a los usuarios.

1.2.4. Protocolos de seguridad integrados en tarjetas de crédito y débito

Silvestre (2021) menciona lo siguiente:

> A través de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, se estipuló que las entidades financieras podían expedir y administrar tarjetas de crédito y débito, razón por la cual con fecha 30 de octubre del 2013, se aprueba la resolución N° 6523-2013 “Reglamento de tarjetas de crédito y débito”, en la cual se consignan las medidas de seguridad. Al ser estas tarjetas un medio de pago de diferentes transacciones comerciales, requieren de medidas de seguridad con la finalidad de resguardar el interés económico del consumidor. (pág. 31)

Dotadas de diversas disposiciones descritas en el artículo decimoquinto del Reglamento de Tarjetas de Crédito y Débito, estas tarjetas cuentan con características únicas como:

> Para que una tarjeta sea reconocida, es fundamental que tenga un chip o circuito integrado incorporado. Estos componentes resultan integrales en el almacenamiento y la supervisión de los datos y la actividad del usuario, alineándose con los estándares

> globales para la funcionalidad y validación de la tarjeta (...)" Según la estipulación típica, los circuitos integrados o chips son obligatorios para estas tarjetas para garantizar las características de seguridad. Los propios chips se consideran inherentes a las medidas de seguridad de las tarjetas, sirviendo como medio para validar operaciones y verificar la autenticación de los pagos. (pág. 31)

Asimismo, Silvestre (2021) señaló que se ha establecido cuatro medidas necesarias:

> Para garantizar la autenticación del usuario, las tarjetas deben cumplir con las normas de seguridad codificadas en sus chips. Además, se debe aplicar un protocolo criptográfico específico para verificar datos y claves. Si se autorizan operaciones fuera de línea, se debe garantizar la seguridad de la tarjeta. Finalmente, en respuesta a las transacciones en línea, los chips de las tarjetas deben incluir mecanismos instructivos que responden al interés y protección al consumidor.

> Las medidas de seguridad antes mencionadas como la verificación de la autenticidad de las tarjetas y la validación de la identidad del usuario asegura el interes del consumidor y su protección económica pretendiéndose dar cumplimiento a lo establecido en el artículo 65° de la Constitución Política del Perú.

1.2.5. Medidas de seguridad respecto a la realización de operaciones en las tarjetas de crédito y débito.

Además de las medidas de seguridad incorporadas en las tarjetas de crédito y débito, el Reglamento del mismo modo regula medidas de seguridad respecto al usuario y a las operaciones que realiza (sistema de monitoreo y alerta). Respecto al usuario, ha normado que las entidades financieras y bancarias deben, como mínimo, entregar la tarjeta al titular, entregar la clave al usuario, permitir su cambio y para los retiros en efectivo se proceda a identificación con riesgo de fraude.

Estas medidas ayudan a la disminución del riesgo de fraude electrónico; sin embargo, estas pueden considerarse evidentes o “naturales” toda vez que, en toda relación de consumo referida a las tarjetas de crédito y débito deberían de darse como forma de concretar una relación de consumo idóneo, así, por ejemplo, es evidente que se deben entregar las tarjetas y clave, así como solicitar su cambio al tarjetahabiente.

El aspecto que adquiere mayor relevancia, son las medidas exigidas para el control del uso de la tarjeta de crédito y débito, a través de la cual, la entidad financiera y bancaria debe detectar las operaciones inusuales en dichas tarjetas analizando su deber de monitoreo para proceder a aplicar las medidas de seguridad**.** Cabe precisar que el funcionamiento del sistema de monitoreo no es predictivo, primero debe de concretarse la operación para que la entidad financiera procese su análisis sobre su inusualidad de acuerdo al patron de consumo del consumidor.

Al respecto, el Reglamento de Tarjetas de Crédito y Débito ha señalado en su artículo 17° las siguientes medidas: (i) la entidad debe contar con un sistema de monitoreo que tendrá como finalidad detectar transacciones que se consideren no usuales, (ii) así mismo debe instaurar un procedimiento para todas las advertencias que se generen en este sistema, (iii) debe identificar los patrones que puedan constituir un fraude, (iv) debe limitar el consumo en caso de alerta, tomando en cuenta que tiene la obligación de reducir las pérdidas por fraude, (v) debe requerir al titular el DNI cuando así se requiera o utilizar cualquier otra forma de identificación para validar la legitimidad del titular y (vi) cuando se efectué algún retiro o cualquier otra operación, debe exigirse la clave de acceso previamente consignada por el titular.

Al exigírsele a las entidades financieras y bancarias contar con un sistema que detecte las operaciones inusuales de las tarjetas y en base a ello implementar un procedimiento para gestionar las alertas emitidas. A través de dicho procedimiento se podrán identificar los patrones de fraude para proceder a limitar y controlar en los canales de atención el consumo evitando más perdidas por el fraude.

La conclusión al que ha arribado la Sala Especializada en Protección al Consumidor es que, la norma ha impuesto una exigencia, que el patrón de consumo que las entidades financieras construyan respecto a los usuarios e integren a su sistema de monitoreo, debe responder a una serie de factores objetivos que la entidad bancaria determine a partir del análisis de la información histórica del usuario.

En mérito a ello, para analizar supuestos de responsabilidad administrativa por consumos inusuales y no reconocidos con tarjetas de crédito o débito, se debe de verificar el monitoreo y detección de operaciones inusuales a cargo del sistema de la entidad financiera y una vez superada dicha evaluación, se procederá a analizar si se realizó un cargo justificado, cumpliendo con los requisitos de validez. (Resolución 0493-2020/SPC-INDECOPI, Fundamento 30).

Entonces, si bien se estipula la obligación a las entidades de adoptar medidas de seguridad frente a operaciones inusuales, sin embargo, la forma en cómo se lleva a cabo este deber de monitoreo no se señala, más aún si el reglamento no estipula la forma en cómo se deben aplicar estas medidas de seguridad, especialmente el de monitoreo y deber de alerta.

Las denuncias administrativas por falta de adopción de medidas de seguridad en las tarjetas de crédito y débitos en especial las que son objeto de estudio, las realizadas por internet, cuestionan por lo general múltiples operaciones realizadas, lo que lleva a evidenciar que la forma en cómo se lleva este monitoreo y aplicación de medidas de seguridad no resultan a la fecha eficientes para proteger los interes económicos del consumidor siendo necesario uniformizar criterios.

Las entidades financieras no actúan de manera rápida frente a las operaciones inusuales, debido a que cada entidad financiera tiene sus propios criterios sobre el deber de monitoreo y alerta, no existiendo criterios establecidos. Esto quiere decir, que el Reglamento de Tarjetas de Crédito y Débito si bien regula la obligación de monitoreo y alerta ante operaciones inusuales, no ha regulado de forma general cómo es que se debe aplicar este mecanismo de seguridad en el sistema financiero.

Con la presente investigación no se pretende indicar que las entidades bancarias y financieras deberían implementar sistemas de seguridad que impidan de manera total cualquier operación inusual; en tanto, ello es imposible hasta el momento, sin embargo si es exigible que la SBS regule cómo aplicar el sistema de monitoreo y alerta de manera preventiva para identificar patrones de fraude de una forma más eficiente y que ante la minina sospecha de una operación inusual, se tomen las medidas correspondientes, evitando así que estas operaciones se concreten en perjuicio de los consumidores.

Es debido a ello, que se debe de evaluar si el sistema de monitoreo y el deber de alerta empleado por las entidades financieras como mecanismo de seguridad para transacciones u operaciones inusuales ante la detección de un riesgo de fraude (operación inusual) deba bloquear de manera inmediata de manera preventiva la tarjeta del cliente enviándole una alerta no para informar sobre si reconoce o no las operaciones, sino, para informar sobre su bloqueo preventivo efectuado, de esta manera evitar que se efectúen operaciones posteriores en salvaguarda de sus intereses económicos.

Con esta premisa se propone un alcance de cómo se debería aplicar las medidas de seguridad en el sistema financiero (sistema de monitoreo y deber de alerta), de tal forma que esta acción garantiza de manera más idónea la protección al consumidor en los servicios financieros.

1.2.6. Educación Financiera

Meza (2012) sostiene lo siguiente:

> En esta era moderna, las tarjetas de crédito son omnipresentes cuando se trata de adquirir mercancías o servicios. Como de costumbre, la gente imprudentemente consigna su firma en el contrato de la tarjeta de crédito sin examinarlo a fondo y, por lo tanto, ignora su responsabilidad de mantenerlo a buen recaudo. En pocas palabras, ignoran el hecho de que usar la tarjeta requiere la tarea de supervisarla, de manera que no vaya a ser víctima de operaciones fraudulentas ya sean físicas o por internet y/o aplicativos móviles. Sin embargo, muchos factores, entre ellos la confianza que se tiene al comprar en un establecimiento, hace que nos descuidemos y que días después (cuando nos llega el estado de cuenta de la tarjeta) nos percatemos que existen consumos que no reconocemos, al haber perdido de vista nuestra tarjeta. (pág. 7)

Actualmente, las tarjetas de crédito se han convertido en una forma efectiva de agilizar las transacciones comerciales, especialmente durante la pandemia; Sin embargo, los mismos avances tecnológicos que nos benefician conllevan una serie de riesgos.

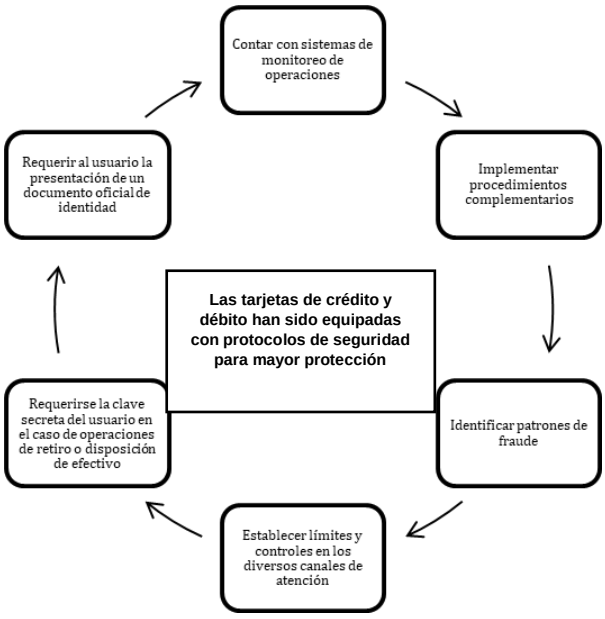
Como afirmó Meza en 2012, el consumo fraudulento es un riesgo potencial asociado al uso de tarjetas de crédito y débito. Dicho consumo se refiere a las compras realizadas por un tercero, que no involucran a las partes originales, pero que son válidas, mientras hayan sido efectuados con los datos sensibles de la tarjeta que es de conocimiento y uso confidencial del tarjetahabiente. (pág. 7)

Con esta premisa de educación financiera de manera previa a la contratacion efectuada a los tarjetahabientes por parte del personal de Banca al momento de la entrega o informada en la contratacion telefónica sobre la no exposición de los datos sensibles de su tarjeta o su deber de comunicar la pérdida o robo de este producto financiero también garantiza de manera más idónea la protección al consumidor en los servicios financieros frente a operaciones no reconocidas tanto por medios virtuales internet como físicas.

1.2.7. Reglamento de tarjetas de crédito y débito de la SBS N° 6523-2013

Las Norma expedida por la Superintendencia de Banca y Seguros, tiene como finalidad reglamentar las tarjetas tanto crédito como la de débito.

En cuanto al seguimiento y realización de las operaciones, la Resolución de la SBS N° 6523-2013 cuenta con el artículo 17° que establece las medidas de seguridad. Indica que la SBS (2013) debe considerar:



Fuente: (Perú, 2013)

2.2.5 Resolución de la SBS N° 5570-2019 que sustituye el numeral 16 del artículo 2, el artículo 3, el artículo 4, los numerales 2, 3, 4, 8, 9 y 12 del artículo 5, el artículo 6, el artículo 7, el primer párrafo del artículo 9, el artículo 10, el primer párrafo del artículo 11, el artículo 13, el primer párrafo del artículo 14, el numeral 4 del artículo 16, el numeral 2 del artículo 22 y el artículo 23.

Artículo 22.- Seguimiento de operaciones que pueden corresponder a patrones de fraude

Para detectar posibles fraudes, las empresas deben establecer procedimientos de seguimiento que cubran, como mínimo, los siguientes aspectos:

(…)

2. Acciones para proceder con el bloqueo temporal o la cancelación definitiva de la tarjeta, en caso sea necesario.

1.3. Definición de términos básicos

Según el Área del Reporte de Estadísticas Institucionales del INDECOPI (2019) se clasifican las siguientes definiciones:

1.3.1. Servicio De Atención al Ciudadano

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (2010) define que:

> "El Servicio de Atención al Ciudadano tiene como objetivo brindar orientación acerca de las funciones, servicios y trámites que son competencia del INDECOPI. Asimismo, es una vía para presentar reclamos cuando, presuntamente, los derechos de un consumidor han sido vulnerados por un proveedor que no le ofrece solución alguna, excepto cuando la competencia de la institución sea negada por norma expresa con rango de ley. Mediante procesos de mediación y conciliación gratuitas, rápidas y sencillas, se busca que el consumidor y el proveedor lleguen a un acuerdo definitivo y satisfactorio para las partes" (pág. 2)

1.3.2. Órganos Resolutivos de Procedimientos Sumarísimos

En 2010, el INDECOPI definió nuevos Órganos de Resolución denominados ORPS. Estos se establecieron para ayudar rápidamente a los consumidores que buscan la resolución célere de sus procedimientos de

denuncias administrativas. El objetivo principal de estos ORPS era atender denuncias de manera célere en merito a sus cortos plazos. (pág. 2)

1.3.3. Comisiones de Protección al Consumidor

El Código de Protección y Defensa del Consumidor está regulado por órganos resolutivos denominados Comisiones de Protección al Consumidor (CPC), según lo señaló INDECOPI en 2010. Solo las denuncias que involucren montos superiores a S/ 13.200 para el 2021, que son superiores a tres UIT, son de competencia del CPC y son revisados por presuntas infracciones a la normativa. (pág. 2)

1.3.4. Sala Especializada en Protección Al Consumidor

La Sala Especializada de Protección al Consumidor (SPC) es el órgano encargado de resolver los casos en materia de protección al consumidor, según la definición de INDECOPI (2010). Resuelven en ultima instancia procedimientos que son conocidos por las comisiones. (pág. 2)

1.3.5. Comportamiento habitual de consumo del usuario

Su estudio de 2021 profundiza en los muchos elementos que afectan las operaciones con tarjetas de usuario. Después de analizar los datos, Pierino, Oscar, José y Antonio destacaron varios factores cruciales: el canal empleado, el lugar de consumo, las categorías de negociación y la frecuencia. Todos estos factores se pueden obtener de los datos de transacción de usuario archivados que almacena la entidad financiera. (pág. 2)

1.3.6. Tarjeta de crédito

Pierino, José; Antonio, Oscar (2021) señalan que:

> Ofrecida ya sea física o digital, la tarjeta de crédito es una herramienta de pago vinculada a una línea de crédito otorgada por la entidad financiera. Según los términos del contrato, los usuarios pueden liquidar deudas por compras, servicios o acceder a servicios complementarios. (pág. 86)

1.3.7. Tarjeta de débito

Pierino, José; Antonio, Oscar (2021) señalan que

> La tarjeta de débito es un instrumento de pago que puede tener soporte físico o representación electrónica o digital, que permite realizar operaciones con cargo a depósitos previamente constituidos en la empresa emisora. A través de la tarjeta de débito el titular puede realizar el pago de bienes, servicios u obligaciones, efectuar el retiro de efectivo o realizar transferencias, a través de los canales puestos a disposición por la empresa emisora u otros servicios asociados, dentro de los límites y condiciones pactados". (pág. 86)

1.3.8. Fraude electrónico

Es definido como la acción que se ha originado ante el avance del internet, este crecimiento ha traído un riesgo de fraude, facilitando los ataques cibernéticos mediante virus; a través de diferentes

estrategias por el defraudador tales como la falsificación de la banda magnética, el cambiazo, la suplantación, el robo y el extravío. (Molano y Correa, 2016).

1.3.9. Operaciones no reconocidas

Las operaciones no reconocidas que son reclamados por los usuarios primero ante la entidad bancaria y si no le dan la solución correspondiente, acuden ante Indecopi para reclamar sobre una operación vía internet que los titulares no realizaron.

Por tal motivo se define como operación no reconocida según el "Reglamento de Tarjetas de Crédito y Débito" (Resolución S.B.S N° 5570-2019) en su artículo 23° menciona que el usuario rechaza la transacción de que tal operación fue realizada incorrectamente. Tales operaciones se pueden realizar de manera presencial o virtual, pero siempre sin el consentimiento del titular; efectuándose a través de páginas web, cajeros automáticos, establecimientos comerciales.

1.3.9.1 Daños que ocasiona las operaciones no reconocidas

Las operaciones que son rechazadas por los usuarios y que han sido efectuadas sin haber adoptado medidas de seguridad por la entidad bancaria, le ocasionan los siguientes daños:

a) **Daños al patrimonio económico:** Se origina este daño, por la conducta del Banco y terceras personas que dispusieron del dinero del consumidor indebidamente, ocasionándole una disminución en su patrimonio. Además, que se invierte tiempo para reclamar por un hecho injusto.

b) **Daño a la persona:** Se ocasiona este tipo de daño cuando el Banco le cobra al usuario por la operación que se ha realizado con la tarjeta mediante internet, no obstante como el usuario rechaza y no paga la deuda que se le imputa, el Banco reporta ante la SBS con calificación como deficiente, lo que le ocasionaría al usuario un daño moral porque al figurar en la central de riesgo, dañaría su imagen como cliente y como consecuencia no podría celebrar transacción alguna con algún otro Banco.

c) **Daños al mercado:** La conducta del Banco al no adoptar las medidas de seguridad y no cumplir con el deber de idoneidad genera una percepción negativa de los consumidores, debido a que pensarían que tener ese sistema de pagos ocasiona un riesgo permanente para su patrimonio, generando desconfianza e inseguridad respectos a las operaciones que se pueden efectuar con estas tarjetas.

1.3.10 Informacion sobre la posición de una de las entidades bancarias que forma parte de la investigación sobre la adopción de medidas de seguridad frente a operaciones no reconocidas por internet .

El INDECOPI a través de la Comisión de Protección al Consumidor N° 3 inició una investigación entre otros, al Banco de Crédito del Perú (en adelante el BCP) a través del cual se le requirió determinada documentación respecto a su deber de monitoreo de operaciones no reconocidas tanto via internet como físicas y conocer como vienen aplicando las medidas de seguridad en relación a las denuncias que se vienen presentando a nivel nacional. Ello, en virtual del Plan anual de Supervisión del año 2021.

El 5 de octubre de 2021, el INDECOPI notificó a BCP la Carta N.º 4256-2021/INDECOPI-DFI, a través de la cual le requirió remitir información sobre

setenta y nueve (79) reclamos encontrados en el PISAC, de acuerdo al siguiente detalle: (i) cuatro (4) reclamos referidos a operaciones no reconocidas: realizadas a través del aplicativo móvil y generada por cuatro (4) consumidores(….)

En atención a ello, el BCP atendió de manera parcial el requerimiento de información, y cuestionó la competencia del INDECOPI para supervisar las acciones realizadas por los proveedores del sector financiero y bancario, el mismo que fue respondido por este ultimo desestimando su cuestionamiento toda vez que los requerimientos de información objeto de análisis fueron formulados en el marco de las competencias que tiene asignadas el Indecopi, como entidad encargada de tutelar y velar por la defensa de los derechos de los consumidores.

Respecto al tema de operaciones no reconocidas, el INDECOPI requirió al BCP que precise y adjunte determinada documentación referida a:

Sobre operaciones no reconocidas

- ✓ Explicar de manera detallada el funcionamiento de los sistemas de monitoreo que emplean para la detección de operaciones fraudulentas o que no correspondan al comportamiento habitual de los consumidores, precisando si el sistema es manual o automático. En cualquiera de los casos deberán señalar cuáles son los pasos que se siguen para la emisión de una alerta; y, el tiempo de duración de cada paso. Asimismo, en caso el sistema de monitoreo sea diferente para operaciones realizadas a través de aplicativos móviles, éste deberá distinguirse y señalarse de manera expresa.
- ✓ Presentar el manual o documento interno que regule el procedimiento del funcionamiento de los sistemas de monitoreo a los que se ha hecho

referencia en el numeral anterior.

- ✓ Indicar si una vez detectada una operación inusual (que no corresponde al comportamiento habitual del consumidor o que presenta características de fraude) proceden al bloqueo preventivo –de manera automática– de la tarjeta o cuenta afectada y/o se comunican directamente con el titular del producto financiero para avisarle de la realización de dichas operaciones. Deberán adjuntar los medios probatorios que consideren pertinentes para acreditar lo indicado, conforme a cada caso en concreto.
- ✓ Precisar y acreditar cómo informan a los usuarios sobre posibles operaciones no reconocidas en las modalidades detalladas en el literal (i) del presente ítem.

a) Respecto de las operaciones que fueron autorizadas a través de aplicativos móviles

Luego de analizar la información que figura en la Pisac, se ha identificado un total de cuatro (4) reclamos por operaciones no reconocidas realizadas a través de aplicativos móviles, los mismos que se detallan en un archivo Excel denominado “Anexo 1 - Universo Operaciones No Reconocidas Aplicativos.xlsx”, y respecto de los cuales requerimos lo siguiente:

- ✓ Presentar copia legible del contrato y demás documentos relacionados a este, suscritos por los usuarios detallados en el Anexo 1.
- ✓ Adjuntar copia de los estados de cuenta de la tarjeta de crédito y/o débito materia de reclamo, correspondientes al período comprendido entre los seis meses anteriores a la fecha en que se

realizó la operación no reconocida de los usuarios detallados en el Anexo 1.

- ✓ Presentar el sustento de su sistema donde conste la autorización de cada uno de los clientes detallados en el Anexo 1 respecto a las operaciones cuestionadas en el reclamo reportado. Para efectos de este requerimiento, deberán describir, detallar y explicar cada número, concepto, campo o carácter que figure en dicho sistema para cada uno de los reclamos.
- ✓ Precisar de manera detallada, de acuerdo con el análisis realizado por su entidad bancaria, cuál es el comportamiento habitual de los usuarios detallados en el Anexo 1, respecto del producto financiero materia de investigación.
- ✓ Precisar si su sistema de monitoreo generó alguna alerta al momento de la realización de las operaciones cuestionadas por los usuarios detallados en el Anexo 1; y, de ser el caso, indicar cuáles fueron las acciones tomadas (comunicación con el cliente, bloqueos preventivos, etc.), debiendo adjuntar los medios probatorios que lo sustenten.
- ✓ En el caso que su sistema de monitoreo no generó alerta alguna o esta fue descartada, señalar qué factores, razones o circunstancias hubieran sido necesarias para que su sistema active o no se descarte una alerta por las operaciones cuestionadas por los usuarios del Anexo 1; debiendo adjuntar los medios probatorios que lo sustente.
- ✓ Explicar y detallar cuáles son los pasos a seguir para realizar la

afiliación al aplicativo, para lo cual, deberá presentar la documentación que lo sustente.

- ✓ Presentar la documentación relacionada a las políticas de uso de los aplicativos móviles puestos a disposición de los consumidores, especificando para ello las medidas de seguridad tomadas en cuenta para dicho uso.
- ✓ Presentar los medios probatorios correspondientes que acrediten que los usuarios detallados en el Anexo 1 se registraron válidamente en el aplicativo.
- ✓ Detallar, describir y explicar: a) los patrones de fraude identificados por su institución y que ha incorporado a su sistema de monitoreo relacionados con el uso de aplicativo móviles; y, b) los límites y controles implementados por su institución respecto a dichas operaciones. Para efectos del presente requerimiento además deberán adjuntar los manuales o documentos internos que regulen estos aspectos.

El BCP en respuesta a todas las interrogantes formuladas por el INDECOPI, atendió de manera parcial el requerimiento según el siguiente detalle:

REQUERIMIENTO DE INFORMACIÓN - CARTA N.° 4256-2021/INDECOPI-DFI		CUMPLIÓ		OSBSERVACIONES
		SI	NO	
Operaciones no Reconocidas (Información referida a 4 reclamos)	(i) Explicar de manera detallada el funcionamiento de los sistemas de monitoreo que emplean para la detección de operaciones fraudulentas o que no correspondan al comportamiento habitual de los consumidores, precisando si el sistema es manual o automático. En cualquiera de los casos deberán señalar cuáles son los pasos que se siguen para la emisión de una alerta; y, el tiempo de duración de cada paso. Asimismo, en caso el sistema de monitoreo sea diferente para operaciones realizadas a través de aplicativos móviles, éste deberá distinguirse y señalarse de manera expresa.		X	No cumplió con señalar de manera expresa si el sistema de monitoreo era diferente para operaciones realizadas a través de aplicativos móviles. No cumplió con precisar de manera expresa si es que su sistema de monitoreo es manual o automático, tampoco ha señalado cuál es el procedimiento y tiempo empleado en cada paso que siguen para emitir una alerta, así como no precisó si su sistema de monitoreo es diferente en el caso de aplicativos móviles, ni precisó la diferencia.
	(ii) Presentar el manual o documento interno que regule el procedimiento del funcionamiento de los sistemas de monitoreo a los que se ha hecho referencia en el numeral anterior.		X	No presentó lo requerido en tanto alegó que era información confidencial. Se informó que en virtud de lo establecido en el inciso 2 del artículo 17 del Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo N.° 021-2019-JUS, la información presentada es declarada confidencial.
	(iii) Indicar si una vez detectada una operación inusual (que no corresponde al comportamiento habitual del consumidor o que presenta características de fraude) proceden al bloqueo preventivo –de manera automática– de la tarjeta o cuenta afectada y/o se comunican		X	No presentó medios probatorios (documentación y/o archivos) que acrediten el procedimiento seguido en ambos casos.

directamente con el titular del producto financiero para avisarle de la realización de dichas operaciones. Deberán adjuntar los medios probatorios que consideren pertinentes para acreditar lo indicado, conforme a cada caso en concreto.				
(iv) Precisar y acreditar cómo informan a los usuarios sobre posibles operaciones no reconocidas en las modalidades detalladas en el literal (i) del presente ítem.			X	No había precisado si los medios de comunicación empleados se utilizaban de manera indistinta o si su uso dependía de un factor determinado. Remitió un ejemplo en el que la transacción fue aprobada y otro en el que se intentó realizar una operación pero la misma fue declinada; motivo por el cual, se le solicitó que precisaran cuándo se procedía a aprobar y cuándo a declinar las operaciones consideradas inusuales, sin embargo no cumplió con atender el pedido.
a) Respecto de las operaciones que fueron autorizadas a través de aplicativos móviles[24]	(i) Presentar copia legible del contrato y demás documentos relacionados a este, suscritos por los usuarios detallados en el Anexo 1.	X		
	(ii) Adjuntar copia de los estados de cuenta de la tarjeta de crédito y/o débito materia de reclamo, correspondientes al período comprendido entre los seis meses anteriores a la fecha en que se realizó la operación no reconocida de los usuarios detallados en el Anexo 1.		X	En referencia al señor [redacted], no presentó el estado de cuenta correspondiente al periodo del 1 al 30 de agosto de 2020. Tampoco señalaron las razones debidamente sustentadas por las que no cumplió con atender dicho requerimiento. Se precisó que en caso de que no se hayan realizado operaciones durante el referido periodo, debía presentar un pantallazo de los movimientos registrados en el que se pueda apreciar las fechas de las operaciones efectuadas por el usuario, pero tampoco cumplió con ello.
	(iii) Presentar el sustento de su sistema donde conste la autorización de cada uno de los clientes detallados en el Anexo 1 respecto a las operaciones cuestionadas en el reclamo reportado. Para efectos de este requerimiento, deberán describir, detallar y explicar cada número, concepto, campo o carácter que figure en dicho sistema para cada uno de los reclamos.		X	Respecto del señor [redacted], presentó información incompleta en cuanto no cumplió con presentar documentación, como por ejemplo, una impresión de pantalla de sus sistemas, en el que se demostrara que para iniciar las operaciones cuestionadas por el usuario se ingresó al aplicativo móvil a través de su número de teléfono autorizado y consignando válidamente su clave de acceso; asimismo, tampoco presentaron documentación que demuestre el ingreso de la claves dinámicas correspondientes en el momento en que se realizaron las transferencias a cuentas de terceros de las 08:25 y 08:29 horas del 20 de enero de 2021. Respecto de la señora [redacted] no presentó la información completa, toda vez que, no adjuntó, como por ejemplo, una impresión de pantalla de sus sistemas, que demostrara que para iniciar las operaciones cuestionadas por la usuaria, se ingresó al aplicativo móvil a través del número de teléfono autorizado consignando válidamente su clave de acceso. El universo en este caso era de 4 consumidores.
	(iv) Precisar de manera detallada, de acuerdo con el análisis realizado por su entidad bancaria, cuál es el comportamiento habitual de los usuarios detallados en el Anexo 1, respecto del producto financiero materia de investigación.		X	En relación a la señora [redacted] sólo presentó documentación del comportamiento habitual en la cuenta [redacted] durante los periodos de marzo, abril, mayo y junio de 2020, pese a que en la documentación remitida se verificó que dicho producto fue contratado el 16 de agosto de 2019 y la operación cuestionada data del 10 de setiembre de 2020. El universo en este caso era de 4 consumidores.

a) Respecto de las operaciones que fueron autorizadas a través de aplicativos móviles[24]	(iv) Precisar de manera detallada, de acuerdo con el análisis realizado por su entidad bancaria, cuál es el comportamiento habitual de los usuarios detallados en el Anexo 1, respecto del producto financiero materia de investigación.		X	En relación a la señora [redacted] sólo presentó documentación del comportamiento habitual en la cuenta [redacted] durante los periodos de marzo, abril, mayo y junio de 2020, pese a que en la documentación remitida se verificó que dicho producto fue contratado el 16 de agosto de 2019 y la operación cuestionada data del 10 de setiembre de 2020. El universo en este caso era de 4 consumidores.
	(v) Precisar si su sistema de monitoreo generó alguna alerta al momento de la realización de las operaciones cuestionadas por los usuarios detallados en el Anexo 1; y, de ser el caso, indicar cuáles fueron las acciones tomadas (comunicación con el cliente, bloqueos preventivos, etc.), debiendo adjuntar los medios probatorios que lo sustenten.		X	-
	vi) En el caso que su sistema de monitoreo no generó alerta alguna o esta fue descartada, señalar qué factores, razones o circunstancias hubieran sido necesarias para que su sistema active o no se descarte una alerta por las operaciones cuestionadas por los usuarios del Anexo 1; debiendo adjuntar los medios probatorios que lo sustente.		X	-
	(vii) Explicar y detallar cuáles son los pasos para seguir para realizar la afiliación al aplicativo, para lo cual, deberá presentar la documentación que lo sustente.	X		
	(viii) Presentar la documentación relacionada a las políticas de uso de los aplicativos móviles puestos a disposición de los consumidores, especificando para ello las medidas de seguridad tomadas en cuenta para dicho uso		X	-
	(ix) Presentar los medios probatorios correspondientes que acrediten que		X	-

Ahora bien, BCP señaló que parte de la información requerida estaba referida a temas confidenciales; sin embargo, la Comisión N° 3 del INDECOPI señaló que ello no justifica la no atención de los requerimientos realizados por la autoridad, pues los administrados tienen la facultad de solicitar la confidencialidad de los mismos-pudo hacerlo, presentar y solicitar que estos sean confidenciales; y la administración por su parte tiene la obligación de resguardar toda aquella información privada que podría afectar los intereses de los proveedores o consumidores, conforme lo establecido en el inciso 2 del artículo 17 del Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo N.º 021-2019-JUS.

En atención a ello, el BCP fue sancionado por el INDECOPI con una multa de 38.35 Unidades Impositivas Tributarias, por infracción de lo establecido en el artículo 5 del Decreto Legislativo N.° 807 - Ley sobre Facultades, Normas y Organización del Indecopi, toda vez que de manera injustificada, incumplió con remitir la información solicitada por la Dirección de Fiscalización a través de la Carta N.° 4256-2021/INDECOPI-DFI del 05 de octubre de 2021 reiterada mediante Carta N.° 5957-2021/INDECOPI-DFI, Carta N.° 0583-2022/INDECOPI-DFI, Carta N.° 0931-2022/INDECOPI-DFI, y, Carta N.° 1597-2022/INDECOPI-DFI., la información obtenida es de acceso público publicada en el repositorio del INDECOPI https://servicio.indecopi.gob.pe/buscadorResoluciones/proteccion-consumidor.seam mediante la RESOLUCIÓN FINAL N.° 010-2023/CC3 de fecha 16 de febrero de 2023, la misma que es apelable y a la fecha en mérito a la apelación interpuesta por el BCP se encuentra pendiente de pronunciamiento.

CAPÍTULO II: OPERACIONALIZACIÓN DE VARIABLES

2.1. Variable Independiente: Medidas de seguridad

Para diseñar una forma efectiva de proteger a los consumidores, se deben tomar mecanismos para minimizar los riesgos que conlleva el uso de tarjetas de crédito y débito. Estos mecanismos se conocen como medidas de seguridad.

2.2. Variable Dependiente: Operaciones por internet

Entre otros canales como aplicaciones móviles y páginas web, estas operaciones se realizan a través de internet y no de manera física con presencia del tarjetahabiente.

2.1. Dimensiones

En la presente investigación, se han identificado dimensiones que permiten evaluar las variables independientes y dependientes.

- **Dimensión 1: Medidas de seguridad incorporadas en las tarjetas.**

  La implementación de medidas en cada tarjeta requiere un chip o circuito integrado capaz de procesar y almacenar la información y las transacciones del usuario, según Alva (2021). Esto facilita una interconexión más rápida y eficiente entre las distintas cuentas financieras cuando se utiliza la tarjeta. Además, la tarjeta está equipada para emitir mensajes de alerta inmediatos si se detecta alguna actividad que amenace los activos del propietario. (pág. 2)

Si un usuario tiene dos tarjetas vinculadas a su cuenta financiera y una de ellas muestra transacciones no autorizadas, tiene la opción de seguir usando la tarjeta válida mientras se investiga la otra tarjeta por actividad fraudulenta. (pág. 2)

La norma de la SBS ha establecido como medida de seguridad inherente a las tarjetas, están los circuitos integrados o chip que cumplan con estándares internacionales de interoperabilidad. La sola consignación del chip, ya se considera una medida de seguridad inherente a estas tarjetas, en tanto a través de las mismas se verifica la validez de las operaciones y autenticación de pagos.

En merito a lo expuesto, el Reglamento de Tarjetas de Creditos y Debitos ha indicado cuatro medidas de seguridad necesarias en las tarjetas, las mismas que servirán para validar la información del usuario; segundo, se debe aplicar cierto procedimiento de criptografía, los cuales estarán destinados a la verificación de datos y claves; tercero, en caso se permita la autorización de operaciones fuera de línea, se debe proporcionar condiciones adecuadas en la seguridad de la tarjeta y finalmente deben existir mecanismos que tenga como fin instruir sobre el chip de las tarjetas en respuesta a transacciones en línea.

- **Dimensión 2: Medidas de seguridad respecto a los usuarios.**

  Además de las medidas de seguridad incorporadas en las tarjetas de crédito y débito, el Reglamento también regula medidas de seguridad respecto al usuario y a las operaciones que realiza (sistema de monitoreo y alerta). Respecto al usuario, ha estipulado que las entidades financieras deben, como mínimo, entregar la tarjeta al titular, entregar la clave al usuario, permitir su cambio y para los retiros en efectivo se proceda a identificación con riesgo de fraude.

De alguna manera estas medidas, también coadyuvan a la disminución en el riesgo de fraude; sin embargo, estas pueden considerarse evidentes o “naturales” toda vez que, en toda relación de consumo referida a las tarjetas de crédito, deben concurrir las mismas como forma de concretar la relación, así, por ejemplo, es evidente que se deben entregar las tarjetas y clave, así como solicitar su cambio.

Por otro lado, el aspecto que adquiere mayor relevancia, son las medidas exigidas para el control del uso de la tarjeta, a través de la cual, la entidad financiera debe reconocer las operaciones inusuales en dichas tarjetas para proceder a aplicar las medidas de seguridad, mediante un sistema de control o monitoreo.

- **Dimensión 3: Medidas de seguridad respecto al monitoreo y realización de operaciones.**

  Según Alva (2021), es su responsabilidad identificar las transacciones que se desvían del comportamiento de consumo habitual de un usuario. Para determinar la regularidad de las operaciones realizadas por cada tarjetahabiente, se deben tomar en cuenta varios factores, como la ubicación, el tipo de negocio, la frecuencia y el canal de uso, lo que se puede conocer a partir de la información histórica registrada de las transacciones de los usuarios (pág. 2)

  La Sala Especializada en Proteccion al Consumidor señala que la norma ha impuesto una exigencia, que el patrón de consumo que las entidades financieras construyan respecto a los usuarios e integren a su sistema de

monitoreo, debe responder a una serie de factores que la entidad bancaria determine a partir del análisis de la información histórica del usuario.

En ese sentido, ante una operación que se considere inusual, la entidad bancaria debe analizar el patrón de consumo a través de su sistema de monitoreo tomando en cuenta la información histórica del cliente y resguardar su interés económico.

Respecto a lo señalado, en un primer momento, para analizar supuestos de responsabilidad administrativa por consumos inusuales y no reconocidos, se verificará el monitoreo y detección de operaciones inusuales a cargo del sistema de la entidad y una vez superada dicha evaluación, se procederá a analizar si se realizó un cargo justificado, cumpliendo con los requisitos de validez. Es obligación del proveedor de servicios financieros identificar patrones de fraude mediante el análisis sistemático de la información histórica de las operaciones". (Resolución 0493-2020/SPC-INDECOPI, Fundamento 30).

Entonces, si bien se estipula la obligación a las entidades de adoptar medidas de seguridad frente a operaciones inusuales, sin embargo, la forma en cómo se lleva a cabo este deber de monitoreo no se señala, más aún si el reglamento no estipula la forma en cómo se deben aplicar estas medidas de seguridad, especialmente el de monitoreo y deber de alerta.

Las denuncias administrativas por falta de adopción de medidas de seguridad en las tarjetas de crédito y débitos en especial las que son objeto de estudio, las realizadas por internet, cuestionan por lo general múltiples operaciones realizadas, lo que lleva a evidenciar que la forma en cómo se lleva este monitoreo y aplicación de medidas de seguridad no resultan a la fecha eficientes para proteger los interes económicos del consumidor siendo necesario uniformizar criterios.

Las entidades financieras no actúan de manera rápida frente a las operaciones inusuales, debido a que cada entidad financiera tiene sus propios criterios sobre el deber de monitoreo y alerta, no existiendo criterios establecidos. Esto quiere decir, que el Reglamento de Tarjetas de Crédito y Débito si bien regula la obligación de monitoreo y alerta ante operaciones inusuales, no ha regulado de forma general cómo es que se debe aplicar este mecanismo de seguridad en el sistema financiero.

Con la presente investigación no se pretende indicar que las entidades bancarias deberían implementar sistemas de seguridad que impidan de manera total cualquier operación inusual; en tanto, ello es imposible hasta el momento, sin embargo si es exigible que la SBS regule cómo aplicar el sistema de monitoreo y alerta de manera preventiva para identificar patrones de fraude de una forma más eficiente y que ante la minina sospecha de una operación inusual, se tomen las medidas correspondientes, evitando así que estas operaciones se concreten en perjuicio de los consumidores.

Es debido a ello, que se debe de evaluar si el sistema de monitoreo y el deber de alerta empleado por las entidades financieras como mecanismo de seguridad para transacciones u operaciones inusuales ante la detección de un riesgo de fraude (operación inusual) deba bloquear de manera inmediata de manera preventiva la tarjeta del cliente enviándole una alerta no para informar sobre si reconoce o no las operaciones, sino, para informar sobre su bloqueo preventivo efectuado, de esta manera evitar que se efectúen operaciones posteriores en salvaguarda de sus intereses económicos.

Con esta premisa se propone un alcance de cómo se debería aplicar las medidas de seguridad en el sistema financiero (sistema de monitoreo y deber de alerta), de tal forma que esta acción garantiza de manera más idónea la protección al consumidor en los servicios financieros.

- **Dimensión 4: Operaciones realizadas a través de internet.**

  Las entidades financieras nos detallan que es un servicio en red que conecta al usuario al sistema de la entidad financiera escogida (de su preferencia) a través de la Internet, este servicio le facilitará realizar las siguientes operaciones:

Servicio Normal	Servicios Especiales
• Consultas de sus cuentas de ahorros. • Consultas de sus cuotas de créditos.	• Transferencias entre sus cuentas de ahorros. • Transferencias a cuentas de terceros. • Pago de cuotas de créditos. • Pago de servicios. • Operaciones frecuentes. • Otros.

“Todas estas operaciones, deberían de ser seguras, ya que viajan a través de un medio encriptado desde su computadora hasta la entidad financiera” (pág. 2).

- **Dimensión 5: Sistemas informáticos que incluye software**

Para mantener la privacidad del titular de la tarjeta, se han creado numerosos sistemas informáticos para limitar la entrada no autorizada y, al mismo tiempo, permitir la comunicación entre su computadora y los servicios aprobados.

Estos criterios van variando en el tiempo y a la vez evolucionan manteniéndose actualizados frente a los ataques de los ciber delincuentes.

Cabe precisar que están diseñados para bloquear, no para eliminar malware o virus que ya se encuentre en el ordenador, debiéndose de usar un antivirus si la finalidad es eliminar.

Las empresas se encuentran en la obligación de implementar medidas de seguridad precisas a la hora de almacenar, procesar y transmitir los datos obtenidos de las tarjetas que han emitido.

- **Dimensión 6: Política de protección contra la vulnerabilidad de las operaciones de Internet**

La continuidad de las operaciones del negocio es un enfoque primordial para las instituciones financieras en la medida en que se garantiza la seguridad de la información, lo cual es posible gracias al cumplimiento de las normas vigentes de la Superintendencia de Banca y Seguros. Estas reglas abarcan tanto la gestión de la seguridad de la información como otros estándares relevantes.

- **Dimensión 7: Se refiere a la eficacia de los protocolos de seguridad**

La minimización del riesgo de uso no autorizado o fraudulento de tarjetas de crédito y débito se logra mediante el uso de medidas de seguridad. Estos componentes clave aseguran la legitimidad de la tarjeta de un usuario, validan su identidad, salvaguardan sus datos personales y autentican los pagos realizados a través de canales electrónicos. Mediante estos mecanismos también se asegura el buen uso de la página y de los canales de acceso.

2.3. Matriz de operacionalización de variables

Tabla 4. Matriz de operacionalización de variables

3.2 Matriz de operacionalización de variables

Tabla 4. Matriz de operacionalización de variables

Variables	Definición conceptual	Definición operacional	Dimensión	Indicadores
Medidas de Seguridad	Son medidas para reducir los riesgos inherentes al uso de tarjetas de débito y crédito y se genere una forma más eficaz de protección al consumidor.	Los mecanismos de seguridad se pueden dimensionar en medidas de seguridad incorporadas en las tarjetas, respecto a los usuarios, respecto al monitoreo y realización de operaciones, en materia de seguridad de la información, en los negocios afiliados.	• Medidas de seguridad incorporadas en las tarjetas	• Grado de eficiencia respecto de las reglas de seguridad definidas en el chip de las tarjetas crédito y débito (en %). • Grado de eficiencia respecto de Procedimientos criptográficos sobre datos críticos (en %). • Grado de eficiencia respecto de Método de autenticación de datos. • Grado de eficiencia respecto de Instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea.

			• Medidas de seguridad respecto a los usuarios	• Grado de eficiencia sobre la Entrega de tarjeta a titular. • Grado de eficiencia respecto al cambo de primera clave o número secreto de la tarjeta. • Grado de eficiencia respecto al Servicio de notificaciones mediante mensajes de texto a un correo electrónico y/o un teléfono móvil, entre otros mecanismos. • Grado de eficiencia respecto de comunicar a la empresa que realizarán operaciones con su tarjeta desde el extranjero.

	• Medidas de seguridad respecto al monitoreo y realización de operaciones	• Grado de eficiencia respecto de los Sistemas de monitoreo de operaciones que detectan operaciones que no corresponden al comportamiento habitual de consumo del usuario. • Grado de eficiencia respecto de la Identificación de patrones de fraude. • Grado de eficiencia respecto de los controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude • Grado de eficiencia respecto de la presentación de un documento oficial de identidad.

Operaciones por internet	Operaciones realizadas a través de internet, desde páginas web y/o aplicaciones de dispositivos móviles, entre otros, distintos a los provistos por la empresa.	Las operaciones por internet se puede dimensionar en operaciones realizadas a través de internet mediante comercio electrónico o transacciones en la web de la entidad financiera.	• Operaciones realizadas a través de internet.	• Grado de eficiencia respecto del Comercio electrónico (internet, aplicativos móviles y otros) • Grado de eficiencia respecto de las Transacciones realizadas en la web de la entidad financiera.

Fuente: Elaboración propia

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Diseño metodológico

El nivel del presente trabajo de investigación fue descriptivo- correlacional

Hernández, Fernández y Baptista (2010), manifiestan que una investigación descriptiva, describe, analiza e interpreta hechos relacionados con las variables tal como se busca especificar las características, propiedades y rasgos relevantes, es decir, estudia su estado actual en su forma natural; donde la posibilidad de tener un control sobre las variables es mínima, por lo cual su validez interna es discutible.

Una investigación correlacional, tiene como fin conocer y evaluar el grado o relación de asociación que existe entre dos o más variables, permitiendo medir a cada una de las variables en estudio, para luego, cuantificar y analizar su vinculación. (Hernández, Fernández y Baptista, 2010).

Hernández y Baptista (2010) indican que las investigaciones que adoptan un enfoque cuantitativo utilizan mediciones numéricas y análisis estadísticos para probar hipótesis y establecer patrones de comportamiento. Este método tiene como objetivo probar teorías basadas en la recopilación de datos. (pág. 4).

En base a lo determinado y a la información recopilada, la presente investigación es cuantitativa, siendo su nivel descriptivo y correlacional. Esto se debe a que el estudio se enfoca en determinar las relaciones entre las variables. Además, es un estudio aplicado con un diseño no experimental y de corte transversal. (pág. 26)

Asimismo, el principal objetivo de la presente investigación fue proporcionar un análisis descriptivo-correlacional. Esto implicó describir tendencias clave dentro de un grupo o población específica, al mismo tiempo que se exploraba la relación y el nivel de asociación entre varios conceptos, categorías o variables dentro de una muestra o contexto determinado. (pág. 26)

Evaluar la relación entre las variables medidas de Seguridad y Operaciones por Internet es el foco principal de este estudio. El tipo de investigación utilizado es el Aplicado, que como transmite Behar Rivero (2008), implica estudiar y aplicar la investigación a problemas distintivos con características y circunstancias específicas. (pág. 26)

Según De Hernández y Baptista (2010), la investigación no experimental implica la observación de fenómenos naturales en su entorno, sin manipulación deliberada de variables. (pág. 114).

En un momento dado, el presente estudio tiene como objetivo evaluar y describir las variables a través de un diseño transversal no experimental que recolecta datos en un solo punto. Su propósito es medir su correlación e impacto. (pág. 26)

3.2. Diseño muestral

3.2.1. Población

La población está compuesta por 1361 colaboradores del INDECOPI conforme a la nómina de personal en el régimen 728 conformada por 621 colaboradores y nómina de personal en el régimen especial (CAS) conformada por 740 colaboradores, según la actualización

al IV Trimestre del año 2021.Respecto a la población se precisa que se esta trabajando con los servidores públicos del INDECOPI de Ica, Tacna y Arequipa conformada por 9 servidores de Ica, 9 de Tacna y 13 de Arequipa.

De las 323 personas que presentaron denuncias ante los Órganos Resolutivos de Procedimientos Sumarísimos del INDECOPI ubicados en la zona sur de Ica, Tacna y Arequipa por operaciones no reconocidas realizadas con tarjetas de crédito y débito, la población usuaria objetivo está conformada por ellas. Específicamente, en este grupo se incluyen 72 personas que presentaron denuncias por este hecho en Ica, 49 de Tacna y 202 de Arequipa.

3.2.2. Muestra

Ante las transacciones en línea utilizando tarjetas de crédito y débito, se analizó a través de de una encuesta directa las percepciones de los servidores públicos respecto a las medidas de seguridad adoptadas por las entidades financieras.

Parte de los empleados públicos de la zona sur del INDECOPI son objeto de una encuesta, según la población objetiva. Este cuestionario se aplicó a 9 servidores públicos de Ica, 9 de Tacna y Arequipa emplea a 13.

De las 323 personas que presentaron denuncias ante los Órganos Resolutivos de Procedimientos Sumarísimos del INDECOPI ubicados en la zona sur de Ica, Tacna y Arequipa por operaciones no reconocidas realizadas con tarjetas de crédito y débito, la población usuaria objetivo

está conformada por ellas. Específicamente, en este grupo se incluyen 72 personas que presentaron denuncias por este hecho en Ica, 49 de Tacna y 202 de Arequipa.

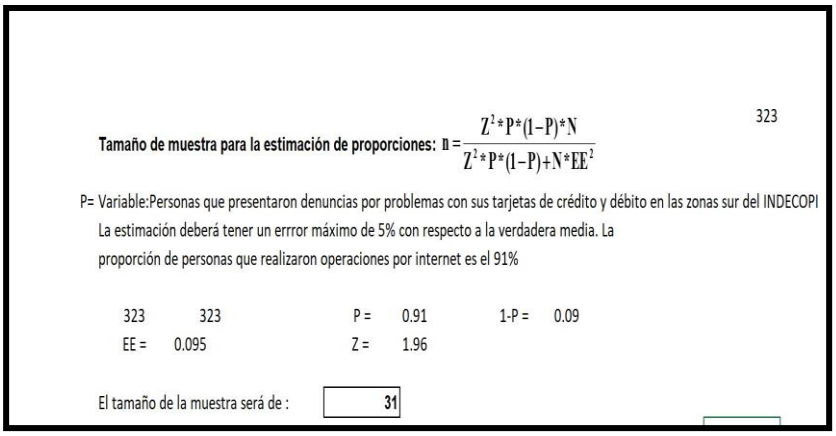
Se estimó encuestar de manera directa y anónima a usuarios de las entidades bancarias que presentaron denuncias ante los ORPS de Ica, Tacna y Arequipa sobre el tema materia de investigación debido que es esta población la que ha sufrido afectación por fraude electrónico con sus tarjetas de crédito o débito, así como también para determinar su grado de conocimiento de educación financiera.

Asimismo se estimó encuestar de manera directa y anónima a los servidores públicos de las oficinas regionales del INDECOPI de Ica, Arequipa y Tacna toda vez que tienen a su cargo el analisis las diversas denuncias que ingresan sobre el tema objeto de investigación aplicando medidas correctivas e imponiendo sanciones administrativas ante su incumplimiento y conocen de primera fuente si las entidades financieras y bancarias vienen aplicando de manera idónea las medidas de seguridad que implementaron para las tarjetas de crédito y débito en cumplimiento de la Resolución SBS 6523-2013.

Una fórmula muy extendida que orienta sobre el cálculo del tamaño de la muestra para datos globales es la siguiente respecto de los usuarios que denunciaron por operaciones no reconocidas con su tarjeta de crédito y débito .

La muestra fue calculada mediante la fórmula de muestreo probabilístico, como se puede apreciar a continuación:

$$n = \frac{Z^2 pqN}{E^2(N-1) + Z^2 pq}$$



Tamaño de muestra para la estimación de proporciones: $n = \frac{Z^2 * P*(1-P)*N}{Z^2 * P*(1-P)+N*EE^2}$ 323

P= Variable:Personas que presentaron denuncias por problemas con sus tarjetas de crédito y débito en las zonas sur del INDECOPI
La estimación deberá tener un errror máximo de 5% con respecto a la verdadera media. La
proporción de personas que realizaron operaciones por internet es el 91%

323	323	P =	0.91	1-P =	0.09
EE =	0.095	Z =	1.96		

El tamaño de la muestra será de : 31

Dónde:

N	=		Población
p	=	0,104	Probabilidad de ocurrencia.
q	=	0,896	Probabilidad de no ocurrencia.
α	=	0,05	Nivel de significación al 95% de confianza
Z	=	1,96	Coeficiente al 95% de confianza
E	=	0,05	Error

N: es el tamaño de la población o universo (número total de posibles encuestados).

Zα: es una constante que depende del nivel de confianza que asignemos. El nivel de confianza indica la probabilidad de que los resultados de nuestra investigación sean ciertos: un 95,5 % de confianza es lo mismo que decir que nos podemos equivocar con una probabilidad del 4,5%. Los valores de Zα se obtienen de la tabla de la distribución normal estándar N(0,1).

3.3. Técnicas de recolección de datos

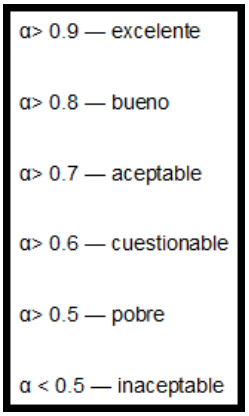
La Técnica de recolección de datos se realizó a través de un cuestionario diseñado con respuestas en escala de Likert, y este cuestionario se aplicó en forma de encuesta directa tanto a los servidores públicos de las oficinas del INDECOPI Ica, Tacna y Arequipa como a los Usuarios que utilizan las tarjetas de crédito y débito que presentaron denuncias sobre el tema de investigación ante el INDECOPI de la zona sur del Perú.

Se eligió la escala de Likert, ya que es una escala de calificación que se utiliza para cuestionar a una persona sobre su nivel de acuerdo o desacuerdo con una declaración, siendo ideal para medir reacciones, actitudes y comportamientos de una persona.

A diferencia de una simple pregunta de «sí» / «no», la escala de Likert permite a los encuestados calificar sus respuestas. Nos sirve principalmente para realizar mediciones y conocer sobre el grado de conformidad de una persona o encuestado hacia determinada oración afirmativa o negativa.

La validación del instrumento se realizó mediante el juicio de tres expertos, y su confiabilidad se midió a través del alfa de Cronbach que es un indicador que mide la confíabilidad de la consistencia interna de un cuestionario, en el presente caso respuestas en escala de Likert, es decir si las preguntas están bien planteadas o no.

La interpretación del valor del coeficiente varía de 0 a 1. Su valor determina el alcance de su significado:



Se obtuvo un valor de 0,74 luego de calcular el coeficiente Alfa de Cronbach, lo que significa que el instrumento utilizado para la investigación es aceptable. Esta información resulta útil ya que el instrumento se puede utilizar en el estudio.

Alfa de Cronbach	N de elementos
0.740	27

3.4. Técnicas de gestión y estadísticas para el procesamiento de la información

La secuencia de actividades para el procesamiento de la información de la investigación se realizó en el siguiente orden:

a) Se procesaron los resultados de los cuestionarios aplicados en una base de datos.

b) El análisis de los datos se realizó con el software estadístico SPSS.

c) A través de tablas y gráficos se presentaron los resultados.

d) Se elaboraron las conclusiones y recomendaciones finales de la investigación.

3.5. Aspectos éticos

Se tuvo en consideración que cada respuesta obtenida fue tratada de manera confidencial y dirigida al proyecto de investigación. Asimismo, los datos obtenidos no serán manipulados o adulterados, de forma que no se considere como plagio de otro proyecto, para que de esa manera lo den un adecuado uso para posteriores investigaciones.

Confidencialidad: De esta forma se asegura la protección de la identidad de la institución y de las personas que participen como informantes de la investigación.

Objetividad: El análisis de la situación encontradas se basan en criterios técnicas e imparciales.

Originalidad: Se tiene en consideración las fuentes bibliográficas de la información mostrada, a fin de demostrar la inexistencia del plagio intelectual.

Veracidad: La información mostrada será verdadera, cuidando la confidencialidad de estas personas o instituciones.

CAPÍTULO IV: RESULTADOS Y PROPUESTA DE VALOR

4.1. RESULTADOS

Para hacer el análisis de los resultados se procederá de la siguiente manera. En primer lugar, se explicará lo concerniente a las medidas de seguridad (variable independiente). Para ello se desarrolla por cada indicador el análisis correspondiente. A continuación, se explicará lo referente a las operaciones por internet (variable dependiente o relacionada). Finalmente, se expondrá la investigación tomando en cuenta cada uno de los objetivos.

4.1.1. Análisis de resultados para la variable medidas de seguridad

4.1.1.1. Dimensión medidas de seguridad incorporadas en las tarjetas

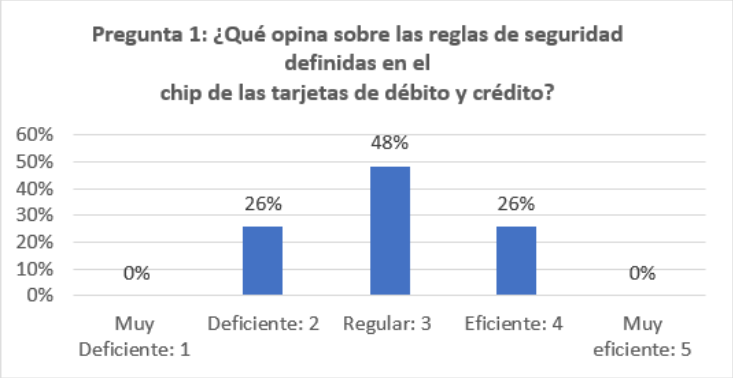
Grado de eficiencia respecto de las reglas de seguridad definidas en el chip de las tarjetas de débito y crédito

Al preguntársele a los servidores públicos del INDECOPI de Arequipa, Tacna e Ica, respecto a las reglas de seguridad definidas en el chip de las tarjetas de débito y crédito para realizar las operaciones financieras, el 48% lo calificó de regular, y el 26% de eficiente. Sólo el 26% lo consideró deficiente. Sobre el particular, las tarjetas deberán contar con un circuito integrado o chip que permita almacenar y procesar la información del usuario y sus operaciones, cumpliendo estándares internacionales de interoperabilidad para el uso y verificación de las tarjetas, así como para la autenticación de pagos; para lo cual deberá

cumplirse como mínimo con los requisitos de seguridad establecidos en el estándar EMV, emitido por EMVCo.

Tabla N° 5: Nivel de seguridad en el chip de las tarjetas de débito y crédito.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	7	26%	26%
Regular: 3	15	48%	74%
Eficiente: 4	9	26%	100%
Total	31	100%	



Grado de eficiencia respecto de los procedimientos criptográficos sobre datos críticos

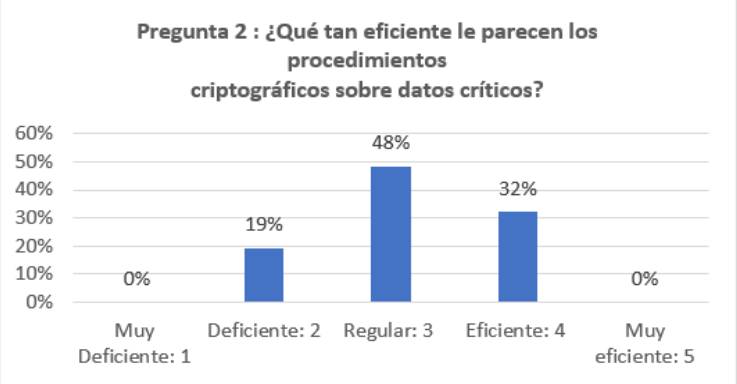
Con respecto al grado de eficiencia para la transferencia segura de información en los procedimientos que son de naturaleza criptográfica, los encuestados del INDECOPI de Ica, Arequipa y Tacna calificaron que las medidas de seguridad relacionadas a los procedimientos criptográficos sobre datos críticos en un 48% es regular, un 32% es eficiente y un 19% es deficiente.

Es importante señalar que, si un intruso viola otros controles de seguridad de red y obtiene acceso a los datos cifrados, sin las claves criptográficas adecuadas no podrá leer ni utilizar esos

datos. Los otros métodos eficaces para proteger los datos almacenados deberían considerarse oportunidades para mitigar el riesgo posible. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos de los titulares de la tarjeta salvo que sea absolutamente necesario, truncar los datos de los titulares de la tarjeta si no se necesita.

Tabla N° 6: **Niveles de eficiencia respecto de los procedimientos criptográficos sobre datos críticos**

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	5	19%	19%
Regular: 3	15	48%	68%
Eficiente: 4	11	32%	100%
Total	31	100%	



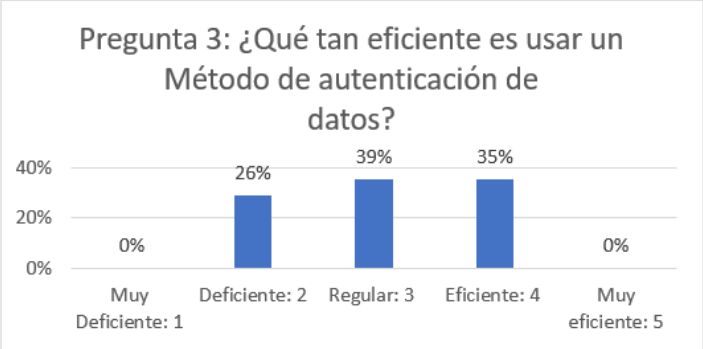
Grado de eficiencia en usar método de autenticación de datos

En relación al grado de eficiencia en usar método de autenticación de datos, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna consideran en un 39% que es regular, en un 35% que es eficiente. Solo el 26% lo consideró deficiente. En otras palabras, además de introducir los datos de nuestra tarjeta de crédito y

débito en posesión (información que sólo el tarjetahabiente posee, tales como el CVV2, la fecha de caducidad, etc), cuando efectuemos operaciones por internet, deben de complementarse con otro factor para su aplicación de una autenticación reforzada como por ejemplo el ingreso de la clave token digital; es valorado por el 35% de los investigados, que le permite generar confianza en sus operaciones.

Tabla N° 7: Niveles de eficiencia en usar métodos autentificación de datos

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	8	26%	29%
Regular: 3	12	39%	65%
Eficiente: 4	11	35%	100%
Total	31	100%	



Grado de eficiencia respecto de las instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea

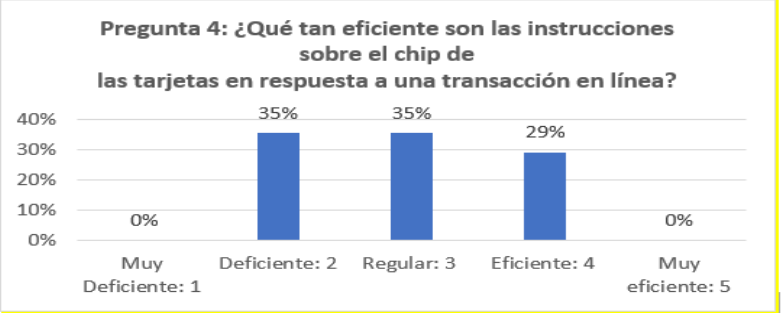
En cuanto al grado de eficiencia respecto de las instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna consideran en un 35% que son regulares, asimismo en un 35% que

son deficientes. Sólo un 29% considera que son eficientes.

Al parecer para el 35% las instrucciones sobre el uso de una tarjeta de crédito o débito las tarjetas con chip siguen siendo propensas a las vulnerabilidades. Por ejemplo, no pueden proteger contra el fraude de tarjeta no presente (Operaciones por internet). Una transacción con tarjeta no presente se produce cuando se paga a distancia sin entrar en contacto con una terminal de punto de venta. Esto puede generar oportunidades que los hackers pueden aprovechar. Todo lo que necesitan son algunos datos de la tarjeta, como el número de la misma, la fecha de caducidad, el código CVV y el tipo de tarjeta. Una vez que tienen esos datos, pueden comprar cosas en Internet. Las tarjetas con chip también utilizan una fuerte encriptación del sistema de punto de venta del comerciante. Cada tarjeta crea un código de transacción único cada vez que se realiza un pago. Este código es decodificado y autentificado por la terminal punto de venta para procesar la transacción. Si la seguridad de la terminal punto de venta es débil, un hacker podría robar la información decodificada y cometer compras no autorizadas. Para evitar esto, se recomienda siempre revisar los estándares de seguridad que tenga la terminal punto de venta que elijas.

Tabla N° 8: Niveles de eficiencia respecto de las instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	11	35%	35%
Regular: 3	11	35%	71%
Eficiente: 4	9	29%	100%
Total	31	100%	



4.1.1.2. Dimensión medidas de seguridad respecto a los usuarios

Grado de eficiencia sobre la entrega de tarjeta a titular

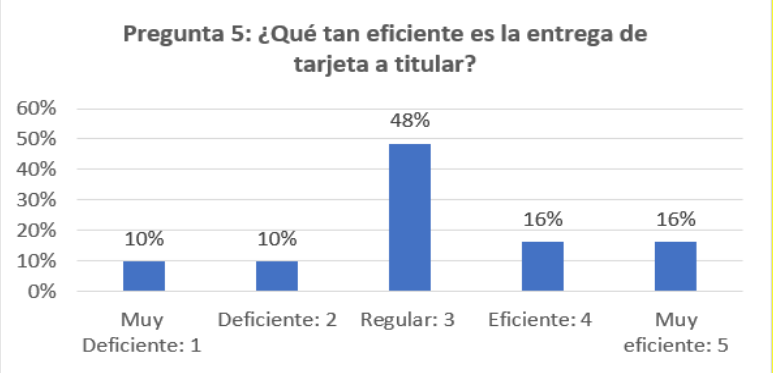
En relación con el grado de eficiencia sobre la entrega de tarjeta a titular; de la población investigada el 16% y 16%, califica como muy eficiente y eficiente respectivamente esta medida. Por otro lado, el 48% lo califica como regular y sólo un 20% como muy deficiente o deficiente.

En otras palabras, han calificado como aceptable esta medida de seguridad referido a entregar la tarjeta y, en caso corresponda, las tarjetas adicionales al titular,

excepto cuando este haya instruido en forma expresa que se entreguen a una persona distinta, previa verificación de su identidad y dejando constancia de su recepción, ya que la posesión de la tarjeta en manos de terceros no autorizados se pueden efectuar operaciones de todo tipo tanto físicas como por internet.

Tabla N° 9: Niveles de eficiencia sobre la entrega de tarjeta a titular

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	3	10%	10%
Deficiente: 2	3	10%	19%
Regular: 3	14	48%	68%
Eficiente: 4	4	16%	84%
Muy eficiente: 5	7	16%	100%
Total	31	100%	



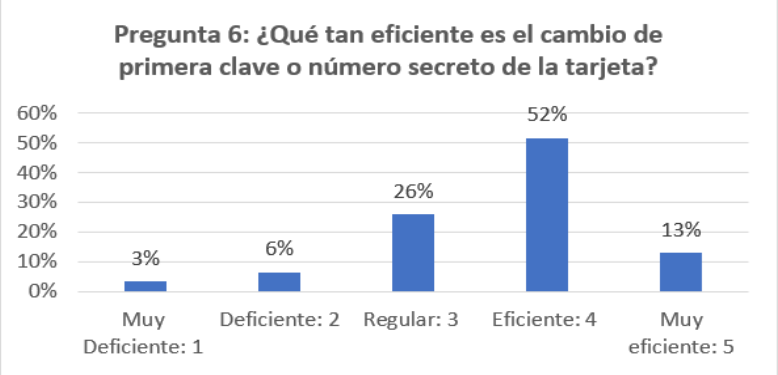
Grado de eficiencia respecto al cambio de primera clave o número secreto de la tarjeta

Respecto al grado de eficiencia al cambiar el código primario o dígito confidencial en una tarjeta, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna: lo califican muy favorablemente. El 52% opina que es eficiente, y el 13% que es

muy eficiente. El 26% señala que es regular y sólo el 9% expresó que es deficiente (6%) o muy deficiente (3%).

Tabla N° 10: **Nivel de eficiencia respecto al cambio de primera clave o número secreto de la tarjeta**

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	2	6%	10%
Regular: 3	7	26%	35%
Eficiente: 4	16	52%	87%
Muy eficiente: 5	5	13%	100%
Total	31	100%	



Grado de eficiencia respecto al servicio de notificaciones mediante mensajes de texto, a un correo electrónico y/o un teléfono móvil, entre otros mecanismos.

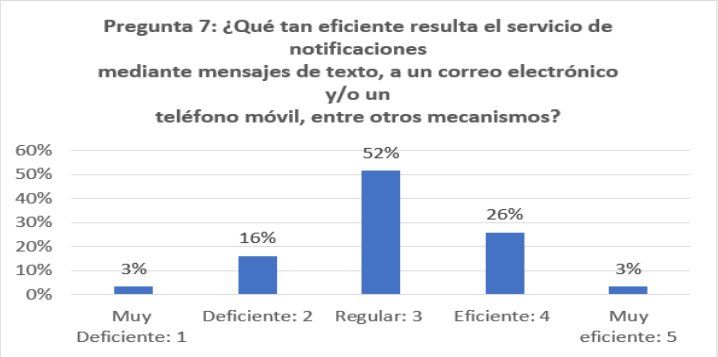
En referencia al grado de eficiencia respecto al servicio de notificaciones mediante mensajes de texto, a un correo electrónico y/o un teléfono móvil, entre otros mecanismos, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna:, lo califican de la siguiente manera: un 52% considera que son regulares, un 29 % considera que son eficientes (26%) o muy eficientes (3%); un 16%

deficientes y sólo un 3% lo valoró como muy deficiente.

Esta medida esta referida para las operaciones de disposición o retiro de efectivo, compras y otras operaciones que la empresa identifique con riesgo de fraude en perjuicio de los usuarios, deberá otorgar a estos la opción de habilitar un servicio de notificaciones que les informe de las operaciones realizadas con sus tarjetas, inmediatamente después de ser registradas por la empresa, mediante mensajes de texto a un correo electrónico y/o un teléfono móvil, entre otros mecanismos que pueden ser pactados con los usuarios.

Tabla N° 11: Nivel de eficiencia respecto al servicio de notificaciones mediante mensajes de texto, a un correo electrónico y/o un teléfono móvil, entre otros mecanismos.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	5	16%	19%
Regular: 3	15	52%	71%
Eficiente: 4	9	26%	97%
Muy eficiente: 5	1	3%	100%
Total	31	100%	



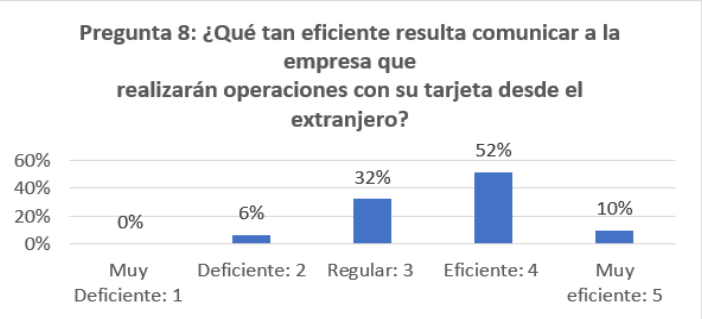
Grado de eficiencia respecto de comunicar a la empresa que realizarán operaciones con su tarjeta desde el extranjero

Los servidores públicos del INDECOPI de Ica, Arequipa y Tacna en cuanto al grado de eficiencia respecto de comunicar a la empresa del sistema financiero que realizarán operaciones con su tarjeta desde el extranjero consideran lo siguiente: un 62% lo califican como eficiente (52%) o muy eficiente (10%). A continuación, el 32% lo valoró como regular. Solo el 6% lo estimó como deficiente.

Las empresas del sistema financiero deben de poner a disposición de los usuarios, la posibilidad de comunicar que realizarán operaciones con su tarjeta desde el extranjero, antes de la realización de estas operaciones y con esta medida ante la omisión del usuario en comunicar, mantener inactiva esta opción.

Tabla N° 12: Niveles de eficiencia respecto de comunicar a la empresa que realizarán operaciones con su tarjeta desde el extranjero

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	4	6%	6%
Regular: 3	8	32%	39%
Eficiente: 4	11	52%	90%
Muy eficiente: 5	8	10%	100%
Total	31	100%	



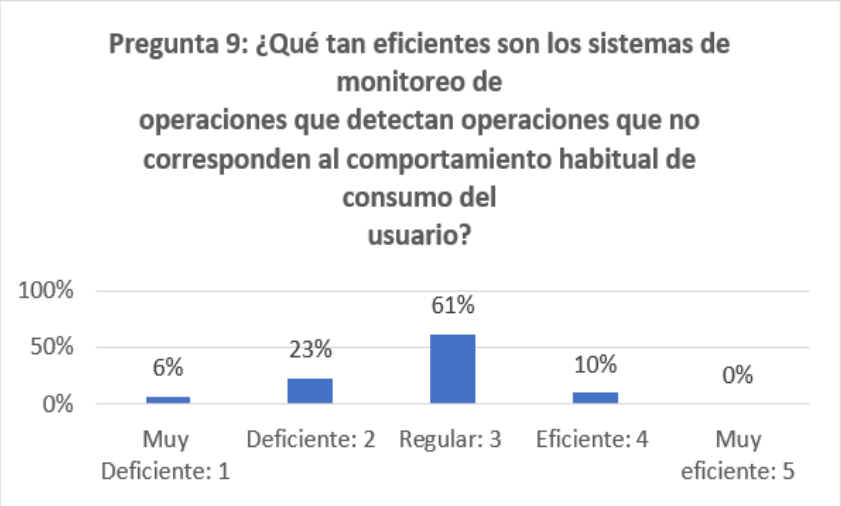
4.1.1.3. Dimensión medidas de seguridad respecto al monitoreo y realización de operaciones

Grado de eficiencia de los sistemas de monitoreo de operaciones que detectan operaciones que no corresponden al comportamiento habitual de consumo del usuario.

Cada cliente tiene un patrón de consumo habitual el cual va creando de acuerdo al historial de operaciones que realiza con una determinada tarjeta de crédito y/o débito. Como medidas de seguridad, es analizado por la entidad financiera a fin de determinar la inusualidad de las operaciones o su carácter de fraudulentas. La evaluación a esta política por los servidores públicos del INDECOPI de Ica, Arequipa y Tacna muestra las siguientes calificaciones: para un 61% es regular, mientras que para el 23% son deficientes. El 10% opinó que es eficiente y el 6%, muy deficiente.

Tabla N° 13: Niveles de eficiencia de los sistemas de monitoreo de operaciones que detectan operaciones que no corresponden al comportamiento habitual de consumo del usuario

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	2	6%	6%
Deficiente: 2	7	23%	29%
Regular: 3	19	61%	90%
Eficiente: 4	3	10%	100%
Total	31	100%	

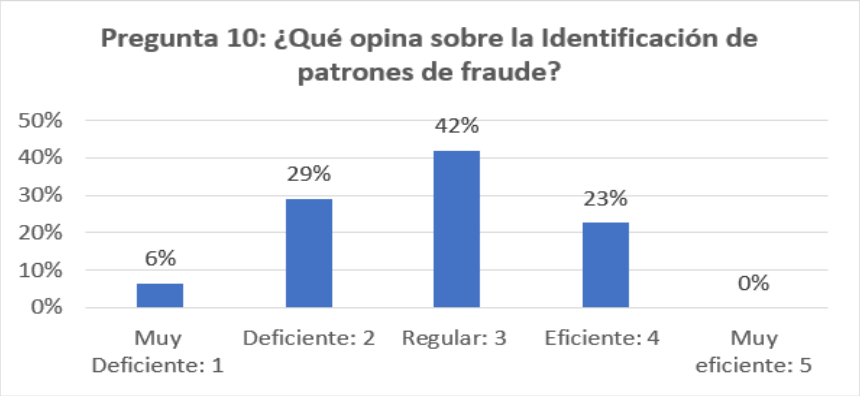


Grado de eficiencia respecto de la identificación de patrones de fraude

En cuanto a la identificación de patrones de fraude, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna lo considera en 42% regular, en un 29% deficiente, en un 23% eficiente. Solo en un 6% muy deficiente. Esta medida de seguridad esta referida a que las empresas del sistema financiero tienen la obligación de identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones que debe tener implementado.

Tabla N° 14: Nivel de eficiencia respecto de la identificación de patrones de fraude

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	2	6%	6%
Deficiente: 2	12	29%	35%
Regular: 3	12	42%	77%
Eficiente: 4	5	23%	100%
Total	31	100%	

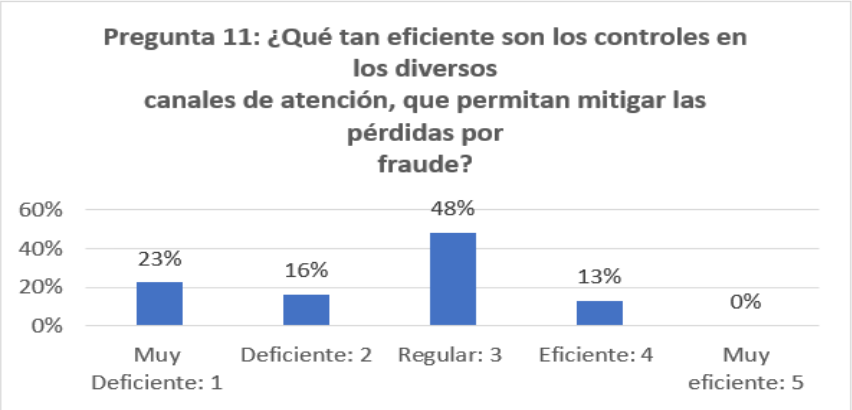


Grado de eficiencia respecto de los controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude.

Los servidores públicos del INDECOPI de Ica, Arequipa y Tacna han determinado que el grado de eficiencia respecto de establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude son: en un 48% regular; seguido de un 39% deficiente (23%) o muy deficiente (16%). Solo en un 13% eficiente.

- Tabla N° 15: Niveles de eficiencia respecto de los controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	7	23%	23%
Deficiente: 2	8	16%	39%
Regular: 3	12	48%	87%
Eficiente: 4	4	13%	100%
Total	31	100%	

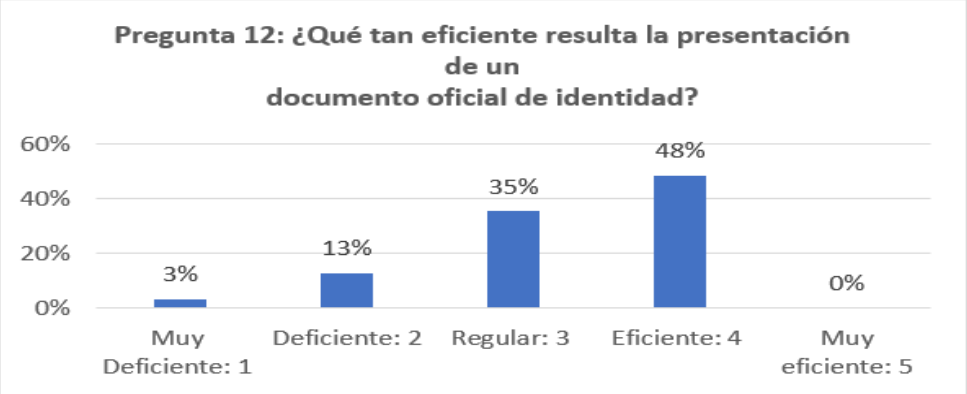


Grado de eficiencia respecto de la presentación de un documento oficial de identidad

Según los servidores públicos del INDECOPI de Ica, Arequipa y Tacna la eficiencia de la medida de seguridad respecto de la presentación de un documento oficial de identidad la califica de la siguiente manera; en un 48 % eficiente, seguido de un 35% regular y el 26% lo califica como deficiente (13%) o muy deficiente (3%). Esta medida de seguridad esta referida a los establecimientos comerciales donde se efectúen operaciones físicas, que deben de solicitar al portador de la tarjeta la presentación del DNI para efectuar operaciones con tarjetas de crédito.

Tabla N° 16: Niveles de eficiencia en la presentación de un documento oficial de identidad.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	7	13%	16%
Regular: 3	10	35%	52%
Eficiente: 4	13	48%	100%
Total	31	100%	



4.1.2. Análisis de resultados para la variable dependiente: operaciones por Internet

4.1.2.1. Dimensión sistemas informáticos que incluye software

Grado de configuración de cortafuegos o firewalls, enrutadores y equipos similares

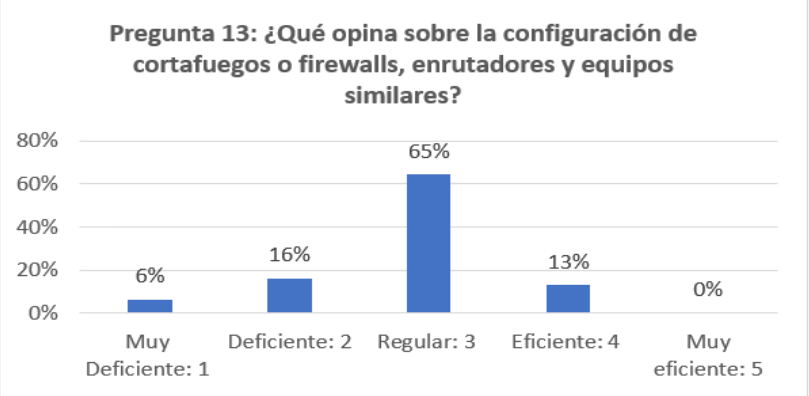
Los servidores públicos del INDECOPI de Ica, Arequipa y Tacna consideran respecto al grado de configuración de cortafuegos o firewalls, enrutadores y equipos

similares que estos son: en un 65% regular; seguido de un 22% deficiente (16%) o muy deficiente (6%). Solo en un 13% eficiente.

Es preciso señalar que en torno al almacenamiento, procesamiento y transmisión de los datos de las tarjetas que emitan, las empresas deben de implementar controles específicos, como, por ejemplo: Implementar y mantener la configuración de cortafuegos o firewalls, enrutadores y equipos similares que componen la red interna, adoptando configuraciones estandarizadas y restringiendo permisos para evitar accesos no autorizados.

Tabla N° 17: Niveles de eficiencia de configuración de cortafuegos o firewalls, enrutadores y equipos similares

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	3	6%	6%
Deficiente: 2	6	16%	23%
Regular: 3	18	65%	87%
Eficiente: 4	4	13%	100%
Total	31	100%	

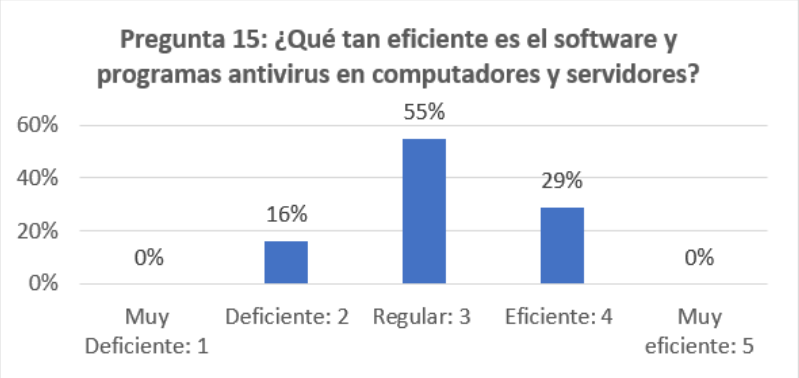


Grado de eficiencia del software y programas antivirus en computadores y servidores

En relación al grado de eficiencia del software y programas antivirus en computadores y servidores, en la evaluación de los parámetros de seguridad predeterminados de los proveedores de servicios de tecnología y el uso de claves secretas los servidores públicos del INDECOPI de Ica, Arequipa y Tacna lo han considerado en un 55% como regular, un 29% como eficiente, un 16% como deficiente

Tabla N° 18: Niveles de eficiencia del software y programas antivirus en computadores y servidores

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	0	0%	0%
Deficiente: 2	6	16%	16%
Regular: 3	15	55%	71%
Eficiente: 4	10	29%	100%
Total	31	100%	



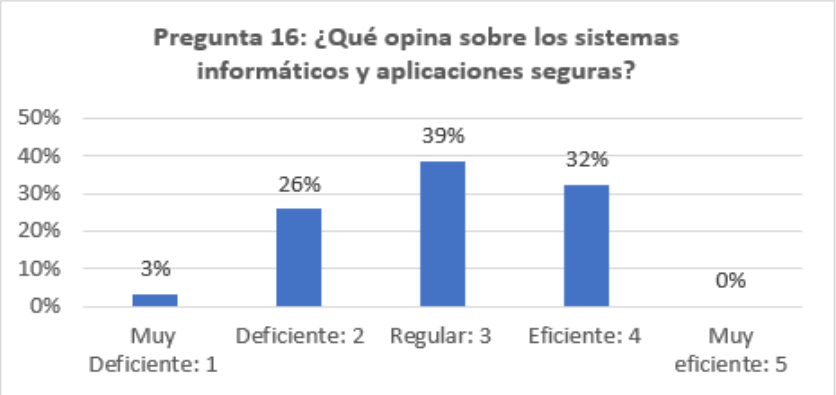
Grado de eficiencia de los sistemas informáticos y aplicaciones seguras para las operaciones por internet.

Los servidores públicos del INDECOPI de Ica, Arequipa y Tacna han determinado respecto al grado de eficiencia de los sistemas informáticos y aplicaciones seguras antivirus para las operaciones por internet que estos son: en un 39% regular; en un 32% eficiente, un 26% deficiente y un 3% muy deficiente.

Esta medida esta referida a que las entidades financieras, deben de implementar controles de seguridad, como es mantener sistemas informáticos y aplicaciones seguras; para el caso de software provisto por terceros, establecer procedimientos para identificar vulnerabilidades y aplicar actualizaciones; para el caso de desarrollos de sistemas propios, adoptar prácticas que permitan reducir las vulnerabilidades de seguridad de dichos sistemas.

Tabla N° 19: Niveles de eficiencia de los sistemas informáticos y aplicaciones seguras para las operaciones por internet

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	8	26%	29%
Regular: 3	12	39%	68%
Eficiente: 4	10	32%	100%
Total	31	100%	



4.1.2.2. Dimensión: Política de protección de la información del tarjetahabiente frente a la vulnerabilidad de la realización de operaciones por internet

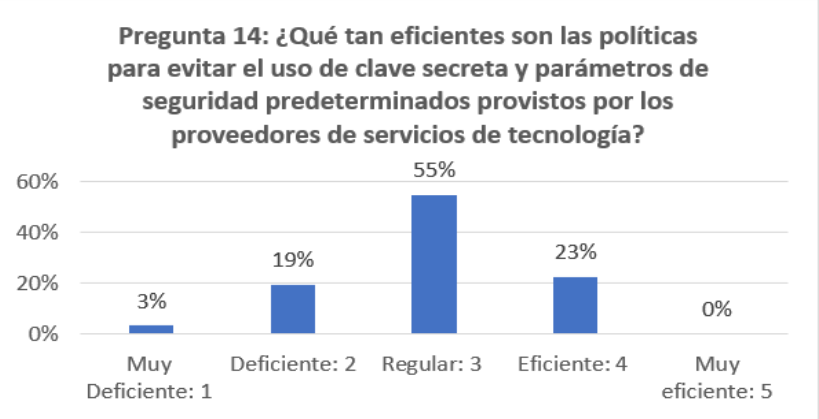
Grado de eficiencia de las políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados provistos por los proveedores de servicios de tecnología.

En relación al grado de eficiencia de las políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados provistos por los proveedores de servicios de tecnología, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna consideran en un 55% que es regular, seguido de un 23% que lo considera

eficiente. De la misma manera, un 22 % lo considera deficiente (19%) o muy deficiente (3%). Esta medida se encuentra referida al cambio de clave las veces que el usuario lo considere conveniente, y el cambio de la primera clave predeterminada por la entidad financiera

Tabla N° 20: Niveles de eficiencia de las políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados provistos por los proveedores de servicios de tecnología

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	7	19%	23%
Regular: 3	16	55%	77%
Eficiente: 4	7	23%	100%
Muy eficiente: 5	0	0%	100%
Total	31	100%	



Grado de eficiencia de las políticas que restrinjan el acceso a los datos de los usuarios solo al personal autorizado, reduciéndolo al estrictamente necesario.

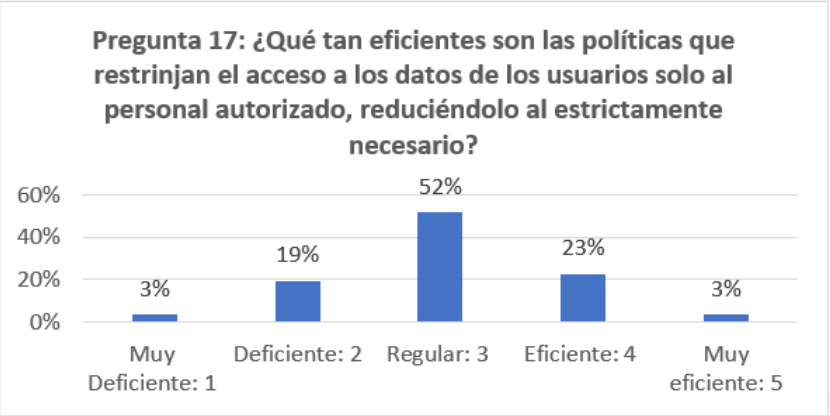
En referencia al grado de eficiencia de implementar políticas que

restrinjan el acceso a los datos de los usuarios solo al personal autorizado, reduciéndolo al estrictamente necesario, los servidores públicos del INDECOPI de Ica, Arequipa y Tacna consideran en un 52% que es regular, en un 22% lo considera eficiente (23%) o muy eficiente (3%) y finalmente en un 22 % que es deficiente (19%) o muy deficiente (3%).

Esta medida se encuentra referida a que las entidades financieras deben de implementar políticas que asegure que los datos financieros de sus tarjetahabientes no se encuentren expuestos, que solo el personal autorizado tengan acceso a ello y cuando sea estrictamente necesario.

Tabla N° 21: **Niveles de eficiencia de las políticas que restrinjan el acceso a los datos de los usuarios solo al personal autorizado, reduciéndolo al estrictamente necesario.**

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	6	19%	23%
Regular: 3	15	52%	74%
Eficiente: 4	7	23%	97%
Muy eficiente: 5	2	3%	100%
Total	31	100%	



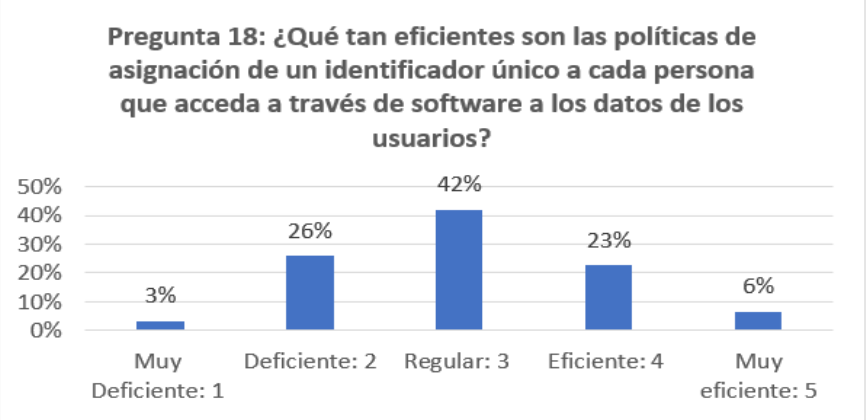
Grado de eficiencia de las políticas de asignación de un identificador único a cada persona que acceda a través de software a los datos de los usuarios.

En referencia al grado de eficiencia de las políticas de asignación de un identificador único a cada persona que acceda a través de software a los datos de los usuarios, los colaboradores encuestados del INDECOPI de Ica, Arequipa y Tacna consideran en un 42% que es regular, seguido de un 29 % que lo consideró eficiente (23%) o muy eficiente (6%). Sólo un 29% lo calificó como deficiente (26%) o muy deficiente (3%). A través de esta medida, las entidades financieras pueden identificar quienes acceden de manera no autorizada a los datos

de los tarjetahabientes.

Tabla N° 22: Niveles de eficiencia de las políticas de asignación de un identificador único a cada persona que acceda a través de software a los datos de los usuarios

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	7	26%	29%
Regular: 3	13	42%	71%
Eficiente: 4	8	23%	94%
Muy eficiente: 5	2	6%	100%
Total	31	100%	



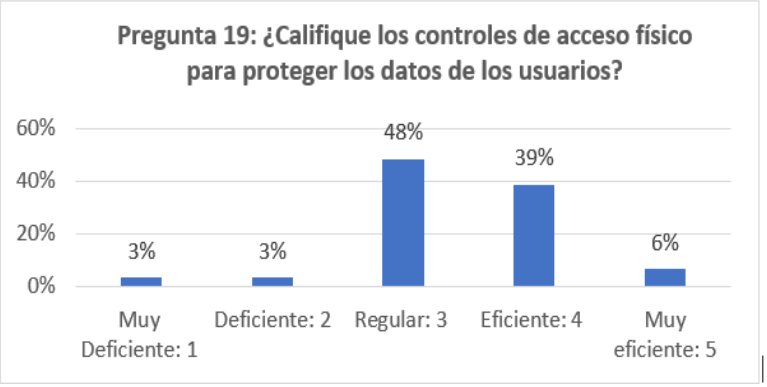
Grado de eficiencia de los controles de acceso físico para proteger los datos de los usuarios.

La población encuestada del INDECOPI de Ica, Arequipa y Tacna opinaron respecto a la medida que tienen los Bancos de implementar controles de acceso físico para proteger los datos de los usuarios, restringiéndolo únicamente a personal autorizado, propio o de terceros lo siguiente: un 48% lo calificó como

regular, un 45% de eficiente (39%) o muy eficiente (6%). Sólo un 6% lo consideró como deficiente (3%) o muy deficiente (3%).

Tabla N° 23: Niveles de eficiencia de los controles de acceso físico para proteger los datos de los usuarios.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	1	3%	6%
Regular: 3	16	48%	55%
Eficiente: 4	11	39%	94%
Muy eficiente: 5	2	6%	100%
Total	31	100%	



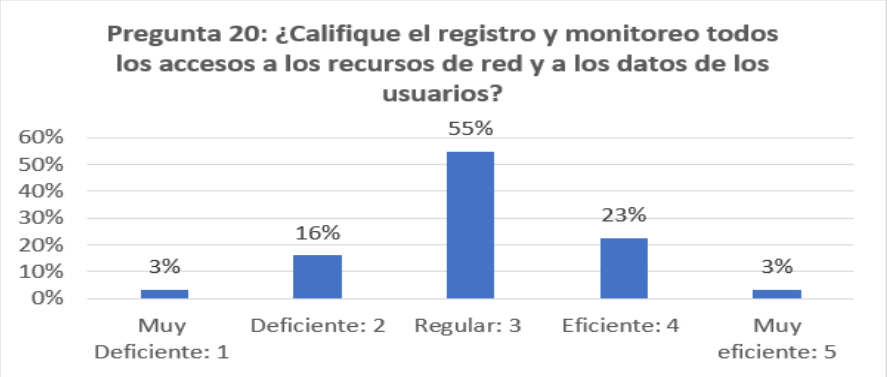
Grado de eficiencia del registro y monitoreo todos los accesos a los recursos de red y a los datos de los usuarios

Los servidores públicos del INDECOPI de Ica, Arequipa y Tacna respecto al grado de eficiencia respecto de registrar y monitorear todos los accesos a los recursos

de red y a los datos de los usuarios, lo califican en un 55% de regular, en un 26% de eficiente (23%) o muy eficiente (3%), mientras que un 19% lo considera como deficiente (16%) o muy deficiente (3%).

Tabla N° 24: Niveles de eficiencia del registro y monitoreo todos los accesos a los recursos de red y a los datos de los usuarios

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	5	16%	19%
Regular: 3	16	55%	74%
Eficiente: 4	7	23%	97%
Muy eficiente: 5	2	3%	100%
Total	31	100%	



4.1.2.3. Dimensión: Relacionado a eficiencia de los mecanismos de seguridad

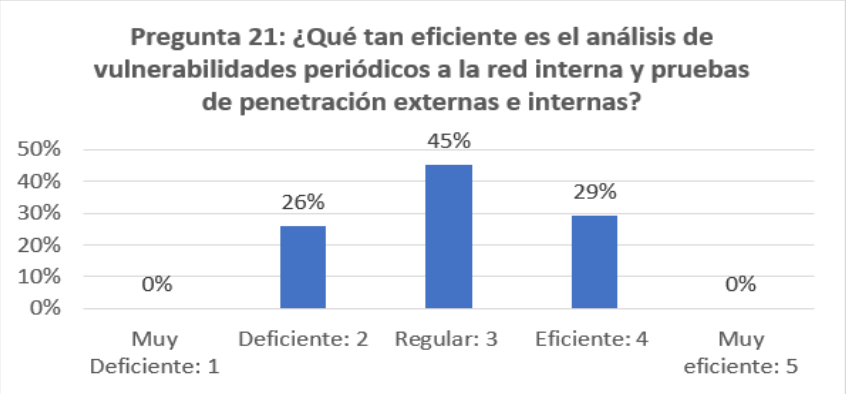
Grado de eficiencia del análisis de vulnerabilidades periódicos a la red interna y pruebas de penetración externas e internas

Respecto a la medida que las empresas del sistema

financiero deben de efectuar un análisis de vulnerabilidades periódicos a la red interna y pruebas de penetración externas e internas, así también luego de cambios significativos en la red o sistemas informáticos, la población encuestada del INDECOPI de Ica, Arequipa y Tacna un 45% lo calificó como regular, seguido de un 29% que lo calificó como eficiente y un 26% considero que es deficiente.

Tabla N° 25: Niveles de eficiencia del análisis de vulnerabilidades periódicos a la red interna y pruebas de penetración externas e internas.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	8	26%	26%
Regular: 3	14	45%	71%
Eficiente: 4	9	29%	100%
Total	31	100%	



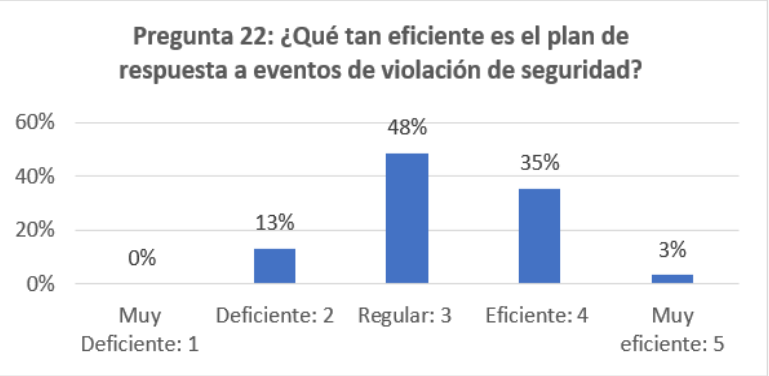
Grado de eficiencia del plan de respuesta a eventos de violación de seguridad

En cuanto al plan de respuesta a brechas de seguridad, los servidores públicos del INDECOPI de Ica, Arequipa

y Tacna han evaluado la medida de seguridad en cuanto a su eficacia. Los resultados indican que el 48% lo encontró regular, el 38% lo calificó como eficiente (35%) o muy eficiente (3%). Sólo el 13% lo calificó de deficiente.

Tabla N° 26: Grado de eficiencia del plan de respuesta a eventos de violación de seguridad.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	0	0%	0%
Deficiente: 2	6	13%	13%
Regular: 3	16	48%	61%
Eficiente: 4	8	35%	97%
Muy eficiente: 5	1	3%	100%
Total	31	100%	



Grado de eficiencia de los procedimientos de aceptación de las operaciones, incluyendo entre otros la verificación de la validez de la tarjeta, la identidad del usuario, y la firma en caso de ser aplicable.

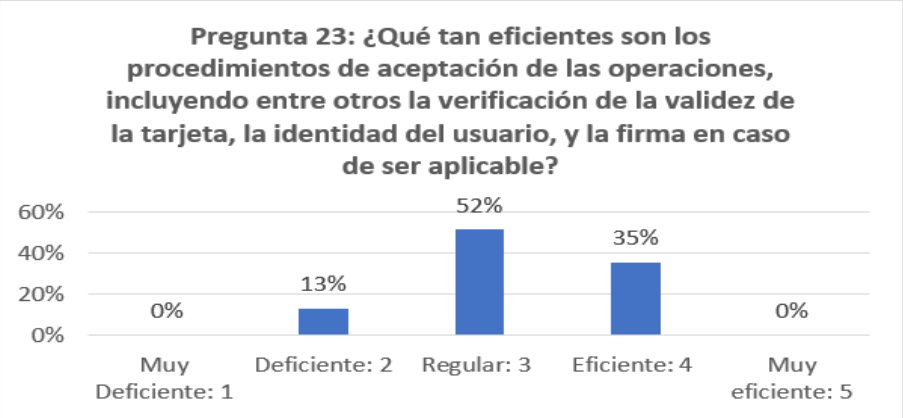
Esta medida se encuentra referida a que las empresas

del sistema financiero deben de asegurarse cuando suscriban contratos con los operadores o establecimientos afiliados, de incluir como obligaciones de estos, de ser el caso, entre otros, la verificación de la validez de la tarjeta, la identidad del usuario, y la firma en caso de ser aplicable.

En base a ello, los encuestados del Indecopi de Ica, Arequipa y Tacna han calificado dichos procedimientos como regular en un 52%, seguido de eficiente en un 35%. Sólo un 13% lo calificó de deficiente.

Tabla N° 27: Niveles de eficiencia de los procedimientos de aceptación de las operaciones, incluyendo entre otros la verificación de la validez de la tarjeta, la identidad del usuario, y la firma en caso de ser aplicable.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Deficiente: 2	5	13%	13%
Regular: 3	16	52%	65%
Eficiente: 4	10	35%	100%
Total	31	100%	

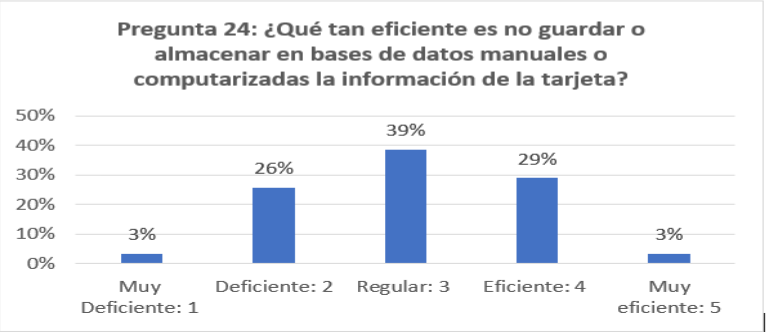


Grado de eficiencia de no guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta

Los encuestados expresaron su opinión sobre las medidas de seguridad en cuanto a la obligación de los establecimientos comerciales en donde se efectúan operaciones físicas, de no guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta, más allá de utilizarla para solicitar la autorización de una operación, con ello evitar su uso fraudulento en la extracción de datos sensibles, dando como resultado que un 39% lo consideró regular, un 32 % lo considero como eficiente (29%) o muy eficiente (3%), mientras que un 29% lo calificó como deficiente (26%) o muy deficiente (3%).

Tabla N° 28: Grado de eficiencia de no guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Muy Deficiente: 1	1	3%	3%
Deficiente: 2	9	26%	29%
Regular: 3	13	39%	68%
Eficiente: 4	7	29%	97%
Muy eficiente: 5	1	3%	100%
Total	31	100%	



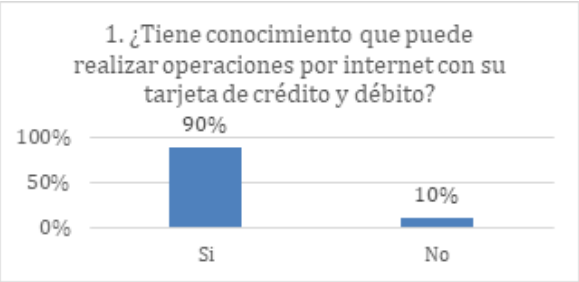
4.1.3. Análisis de resultados para la variable operaciones por internet con tarjeta de crédito y/o débito, desde el punto de vista del usuario.

Grado de conocimiento que pueden realizar operaciones en internet con su tarjeta de crédito y/o débito.

Con respecto al nivel de conocimiento de los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario de tener habilitada dicha opción en sus tarjetas de créditos y débitos. El 90% de los usuarios posee el conocimiento. Sólo un 10% desconoce dicha posibilidad habilitada en sus tarjetas.

Tabla N° 29: **Niveles de conocimiento que pueden realizar operaciones en internet con su tarjeta de crédito y/o débito**

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje
Si	2		
No			
Total			

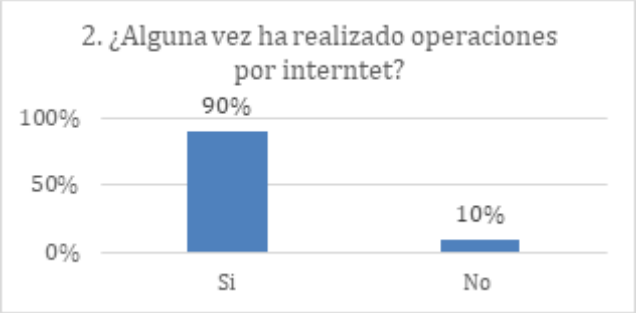


Grado de conocimiento de haber realizado alguna vez operaciones por internet

En relación con el grado de conocimiento de haber realizado alguna vez operaciones por internet esta referido al uso de este canal habilitado, siendo que los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario encuestados ha hecho uso de este canal en un 90%, mientras que un 10% no lo utilizó.

Tabla N° 30: **Conocimiento de haber realizado alguna vez operaciones por internet**

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Si	28	90%	90%
No	3	10%	100%
Total	31	100%	

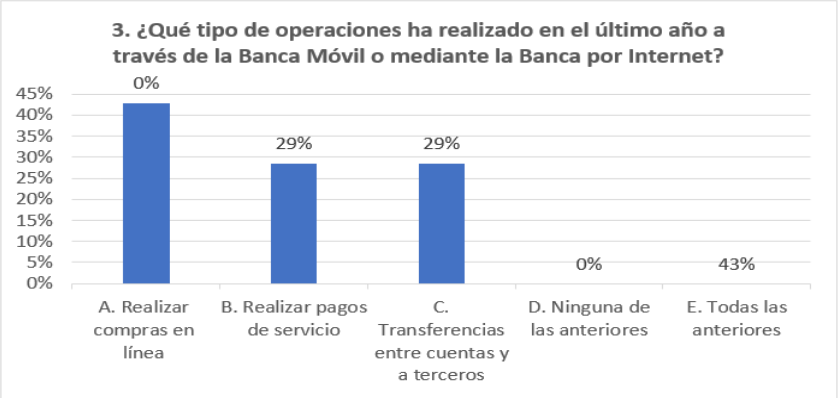


Tipos de operaciones realizadas en el último año a través de la Banca Móvil o mediante la Banca por Internet.

En referencia a los tipos de operaciones realizadas en el último año a través de la Banca Móvil o mediante la Banca por Internet, los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario han señalado en un 43% que han efectuados diversas operaciones en el último año tales como: transferencias a terceros, pagos de servicios, etc. Mientras que un 29% indicó que durante el último año ha efectuado Transferencias entre cuentas y a terceros. Sólo un 29% indicó que realizó pagos de servicios en el último año.

Tabla N° 31: Tipos de operaciones que han realizado en el último año a través de la Banca Móvil o mediante la Banca por Internet.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
B. Realizar pagos de servicio	1	29%	71%
D. Todas las anteriores	18	43%	100%
E. Transferencias entre cuentas y terceros	12	29%	100%
Total	31	100%	

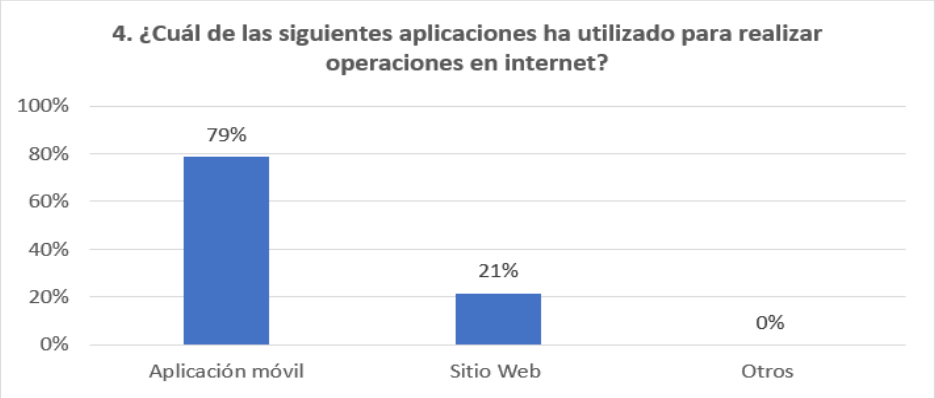


Aplicaciones que han utilizado para realizar operaciones en internet

El 79% de los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario ha utilizado aplicación móvil para realizar operaciones en internet, el el 21% ha utilizado sitio web.

Tabla N° 32: Aplicaciones que han utilizado para realizar operaciones en internet

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Aplicación móvil	14	79%	79%
Sitio Web	6	21%	100%
Otros	11	0%	100%
Total	31	100%	

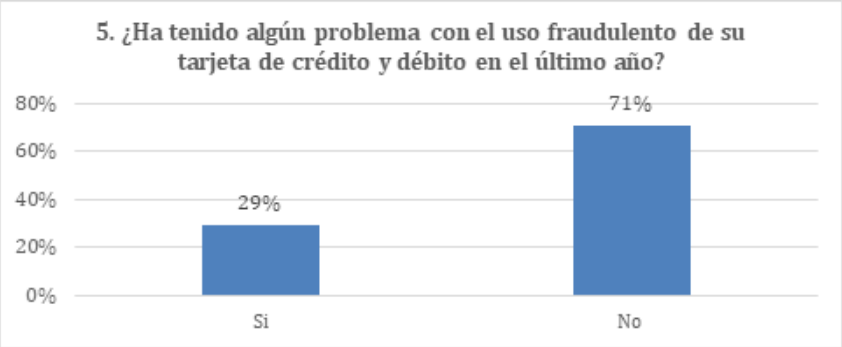


Problema con el uso fraudulento de su tarjeta de crédito y/o débito en el último año.

El 71% de los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario no ha tenido problemas en el último año para realizar operaciones en internet, mientras que el 29% de ellos, presentó problemas en el último año con el uso fraudulento de su tarjeta de crédito y/o débito.

Tabla N° 33: Problema con el uso fraudulento de su tarjeta de crédito y/o débito en el último año.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Si	9	29%	29%
No	22	71%	100%
Total	31	100%	

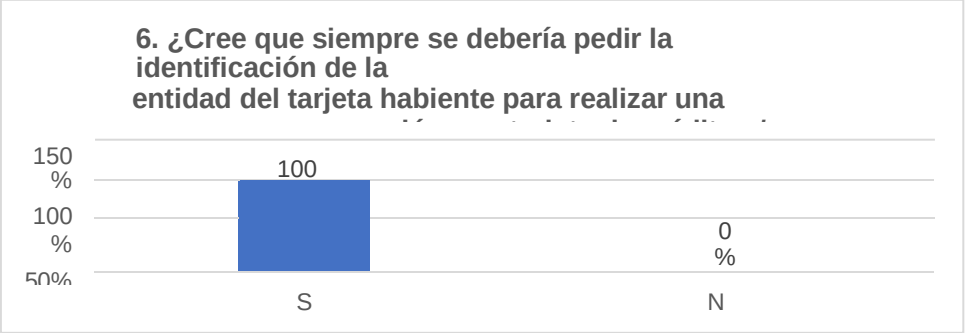


Pedido de identificación de la tarjeta habiente para realizar una operación con tarjeta de crédito

La totalidad de los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario consideran que siempre se debería pedir la identificación del tarjetahabiente para realizar una operación con tarjeta de crédito.

Tabla N° 34: Pedido de identificación del tarjeta habiente para realizar una operación con tarjeta de crédito.

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje
Si	3		
No			
Total			

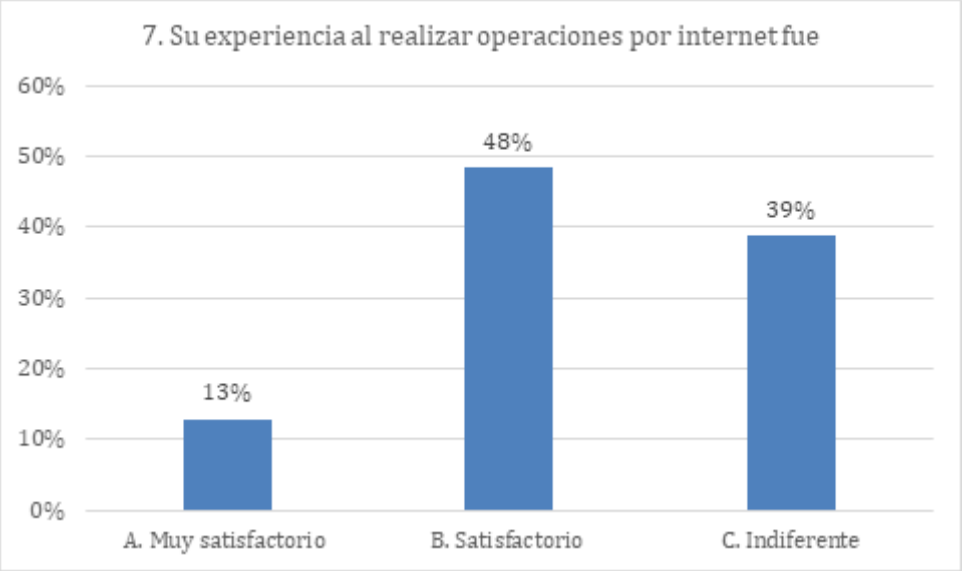


Experiencia al realizar operaciones por internet

El 61% de la población encuestada que utilizan las tarjetas de crédito y débito en el sistema financiero bancario expresan que ha sido muy satisfactoria (13%) o satisfactoria (48%) su experiencia al realizar operaciones por internet. Solo el 39% consideró que le es indiferente dicha experiencia.

Tabla N° 35: Experiencia al realizar operaciones por internet

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
A. Muy satisfactorio	4	13%	13%
B. Satisfactorio	15	48%	61%
C. Indiferente	12	39%	100%
Total	31	100%	

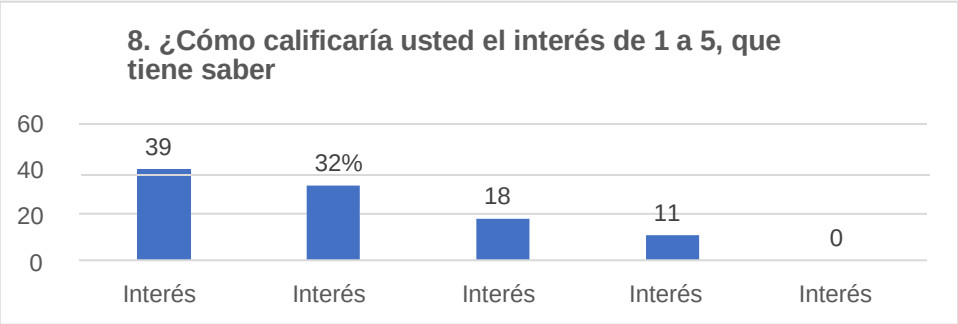


Grado de interés de efectuar operaciones por internet

El 71% de los encuestados que utilizan las tarjetas de crédito y débito en el sistema financiero bancario califica que tiene muy alto (39%) o alto interés (32%) en saber más sobre cómo efectuar operaciones por internet, mientras que un 29% tiene interés bajo (18%) o muy bajo (11%) de conocer más sobre su uso.

Tabla N° 36: Grado de interés de efectuar operaciones por internet

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
Interés 5	11	39%	39%
Interés 4	10	32%	71%
Interés 3	7	18%	89%
Interés 2	3	11%	100%
Interés 1	0	0%	100%
Total	31	100%	

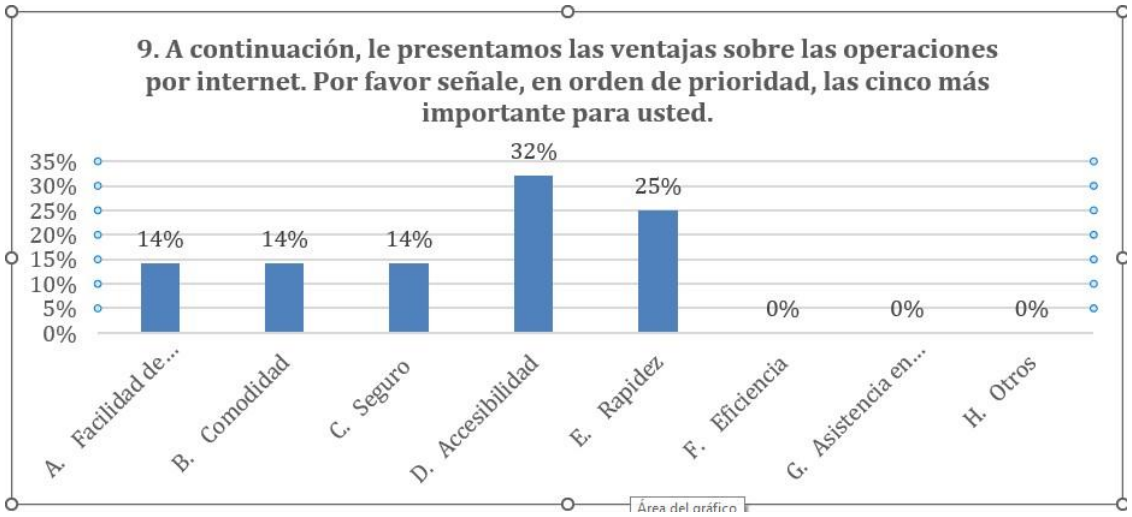


Ventajas sobre las operaciones por internet

El 57% de los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario considera a la accesibilidad (32%) y rapidez (25%) como principales ventajas sobre las operaciones por internet, mientras que el 14% califica la facilidad de uso, la comodidad y la seguridad como una ventaja menor que da las operaciones por internet.

Tabla N° 37: Ventajas sobre las operaciones por internet

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
A. Facilidad de uso	7	14%	14%
B. Comodidad	4	14%	29%
C. Seguro	4	14%	43%
D. Accesibilidad	9	32%	75%
E. Rapidez	7	25%	100%
F. Eficiencia	0	0%	100%
G. Asistencia en la compra	0	0%	100%
H. Otros	0	0%	100%
Total	31	100%	

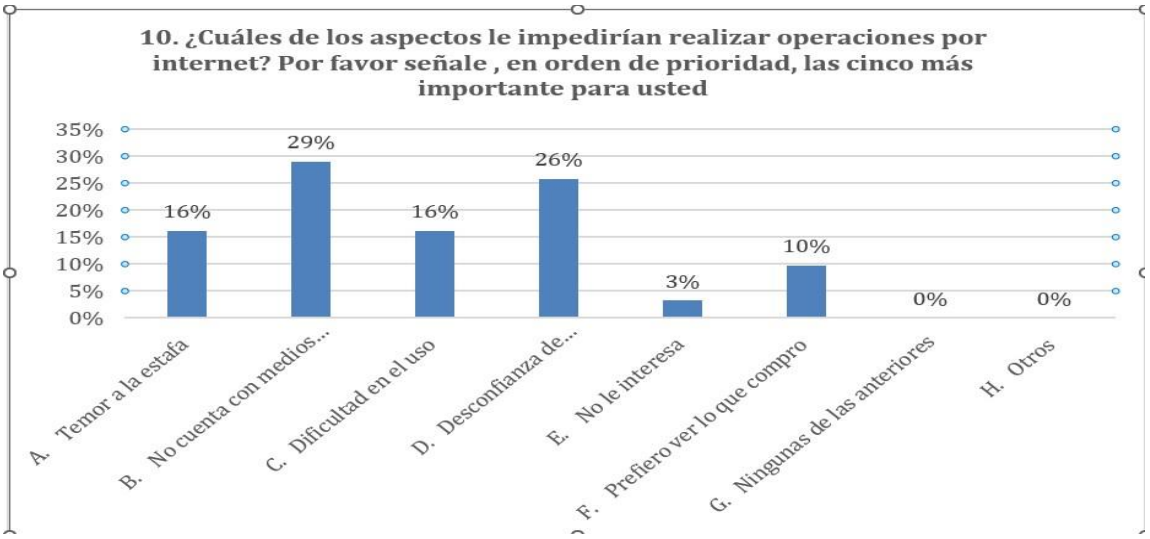


Aspectos que impedirían realizar operaciones por internet

El 29% de los usuarios que utilizan las tarjetas de crédito y débito en el sistema financiero bancario considera que el mayor aspecto que le impedirían realizar operaciones por internet es no contar con los medios necesarios para realizarlas, seguido de un 26% que indica que la desconfianza de proporcionar datos personales es otro de estos aspectos. Asimismo, el 16% califica que el temor a la estafa y la dificultad en el uso, son aspectos que le impedirían realizar operaciones por internet. Sólo un 10% prefiere ver lo que compra y un 3% no le interesa efectuarlas.

Tabla N° 38: Aspectos que impedirían realizar operaciones por internet

Valor Cualitativo	Frecuencia	Porcentaje	Porcentaje Acumulado
A. Temor a la estafa	5	16%	16%
B. No cuenta con medios necesarios	9	29%	45%
C. Dificultad en el uso	5	16%	61%
D. Desconfianza de proporcionar datos personales	8	26%	87%
E. No le interesa	1	3%	90%
F. Prefiero ver lo que compro	3	10%	100%
G. Ningunas de las anteriores	0	0%	100%
H. Otros	0	0%	100%
Total	31	100%	



4.1.4. Resultados en función a los objetivos

Cada una de las dimensiones respectivas se sometió a un análisis utilizando el software SPSS v.26, y los resultados correlacionales se muestran en las tablas a continuación. Para interpretar la relación estadística entre las variables se utilizó la prueba de chi-cuadrado para las dimensiones de cada variable.

4.1.3.1. Respecto al objetivo específico 1

La Tabla 1 revela una correlación entre la protección cibernética de las tarjetas de débito y crédito y el uso de transacciones en línea en Ica, Arequipa y Tacna según los datos de los Órganos Resolutivos de Procedimientos Sumarísimos del INDECOPI de 2021. La prueba de chi-cuadrado reveló un valor p de 0.115, lo que sugiere que P=0,05 no es lo suficientemente bajo como para establecer un vínculo significativo. Las medidas de seguridad incorporadas en las tarjetas de débito y crédito tiene un nivel de confianza del 88,5% en relación al interés de realizar las operaciones por Internet.

Tabla 39: Relación entre las medidas de seguridad incorporadas en las tarjetas de débito y crédito, y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Medidas de seguridad incorporadas en las tarjetas * Operaciones por internet	31	100,0%	0	0,0%	31	100,0%

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	12,923[a]	8	,115
Razón de verosimilitudes	14,118	8	,079
Asociación lineal por lineal	5,748	1	,017
N de casos válidos	31		

a. 13 casillas (86,7%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,29.

Fuente: Encuesta de eficiencia sobre medidas de seguridad para uso de tarjetas de crédito y débito.

Elaboración: Propia

4.1.3.2. Respecto al objetivo específico 2

El interés por realizar operaciones por internet y las medidas de seguridad respecto de los usuarios pueden estar vinculados, como lo demuestran los datos de la Tabla 2. Al analizar los ORPS del INDECOPI en Arequipa, Ica y Tacna para el año 2021, los resultados indicaron una conexión entre las dos variables, determinamos un valor de p de 0,05 después de realizar una prueba de chi cuadrado con un nivel de significación de 0,076. Las operaciones por Internet relacionadas con las medidas de seguridad respecto de los usuarios, tienen un nivel de confianza

del 92,4%. Por lo tanto, se puede concluir que el interés por las medidas de seguridad respecto de los usuarios es importante para dichas operaciones.

Tabla 40: Relación entre las medidas de seguridad respecto a los usuarios y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Medidas de seguridad respecto a los usuarios * Operaciones por internet	31	100,0%	0	0,0%	31	100,0%

Pruebas de chi-cuadrado

	Valor	gl	Sig. Asintótica (bilateral)
Chi-cuadrado de Pearson	15,587[a]	9	,076
Razón de verosimilitudes	16,404	9	,059
Asociación lineal por lineal	8,623	1	,003
N de casos válidos	31		

a. 16 casillas (100,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,16.

Fuente: Encuesta de eficiencia sobre medidas de seguridad para uso de tarjetas de crédito y débito.

Elaboración: Propia

4.1.3.3. Respecto al objetivo específico 3

La correlación entre las medidas de seguridad de monitorear y ejecutar operaciones por internet se reveló en los resultados de la Tabla 3 para los ORPS del INDECOPI de Ica,

Arequipa y Tacna en 2021. Al evaluar la prueba de chi-cuadrado, el resultado tuvo un nivel de significación de 0,033, que cayó por debajo del umbral de p=005. El monitoreo de las operaciones via Internet en cuanto a las medidas de seguridad tiene un nivel de confianza del 95%. Esto confirma la correlación entre monitorear y ejecutar operaciones con un mayor nivel de confianza.

Tabla 41: Relación entre las medidas de seguridad respecto al monitoreo y realización de operaciones, y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Medidas de seguridad respecto al monitoreo y realización de operaciones * Operaciones por internet	31	100,0%	0	0,0%	31	100,0%

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	18,191[a]	9	,033
Razón de verosimilitudes	14,762	9	,098
Asociación lineal por lineal	5,319	1	,021
N de casos válidos	31		

a. 14 casillas (87,5%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,10.

Fuente: Encuesta de eficiencia sobre medidas de seguridad para uso de tarjetas de crédito y débito.

Elaboración: Propia

4.1.3.4. Respecto al objetivo general

En 2021, los ORPS del INDECOPI de Ica, Arequipa y Tacna realizaron un estudio analizando la relacion de las medidas de seguridad para el uso de tarjetas de débito y crédito y el interés a realizar transacciones en línea. Los resultados, que se presentaron de forma descriptiva, revelaron una conexión entre estos factores. La prueba de chi-cuadrado realizada indicó un nivel de significación de 0,039, que está por debajo de p=0,05. En cuanto al uso de tarjetas de débito y crédito, se afirma que el interés de las operaciones por Internet está relacionado con los mecanismos de seguridad que la entidad financiera les ofrece. Esta afirmación está respaldada por un alto nivel de confianza superior al 95%.

Tabla 42: Relación entre las variables: medidas de seguridad respecto al uso de tarjetas de débito y crédito, y el interés en realizar operaciones por internet según los ORPS del INDECOPI de Ica, Arequipa y Tacna

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Mecanismos de seguridad * Operaciones por internet	31	100,0%	0	0,0%	31	100,0%

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	13,300[a]	6	,039
Razón de verosimilitudes	15,919	6	,014
Asociación lineal por lineal	4,569	1	,033
N de casos válidos	31		

a. 11 casillas (91,7%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,52.

Fuente: Encuesta de eficiencia sobre medidas de seguridad para uso de tarjetas de crédito y débito.

Elaboración: Propia

PROPUESTA DE VALOR

Se plantea el reforzarmiento de las medidas de seguridad establecidas en el Reglamento de Tarjetas de Crédito y de Débito en relación a las siguientes propuestas de valor: Se debe de reforzar las medidas de seguridad ya reguladas por la SBS en el articulo 17 del Reglamento de Tarjetas de Crédito y débito en relación a las medidas de seguridad incorporadas en las tarjetas, respecto de los usuarios y respecto al monitoreo y realización de operaciones.

- Respecto a las medidas de seguridad incorporadas en las tarjetas, se propone que se priorice las tarjetas de crédito y débito digitales que ofrecen el CVV dinámico cuya función es proteger sus datos y evitar que sean usados de una segunda vez. Asimismo, se propone que la entidad financiera emisora le expida una tarjeta que no tenga los números al frente para mantener oculta la información sensible a simple vista.

La SBS ha normado las medidas de seguridad respecto al usuario infiriendo que, como mínimo deben de, entregar la tarjeta al titular, entregar la clave al usuario, permitir su cambio y para los retiros en efectivo se proceda a identificación con riesgo de fraude.

- Se propone incidir en la educación financiera si bien en los contratos adhesivos la entidad financiera consigna los derechos y obligaciones, canales de atención, que hacer en caso de perdida, robo, etc de la tarjeta, o mantenerla en custodia, el derecho de activar y desactivar notificaciones de realización de operaciones, servicios adicionales como sobregiros, compras en el exterior, compras por internet, disposición en efectivo; sin embargo, no es menos cierto que la tendencia es no leer lo que se firma,

y en consecuencia no saber que el solo hecho de haber contratado una tarjeta de crédito trae consigo además de beneficios, peligros a los cuales me veo expuesto, si no cumplo con las condiciones de seguridad pactadas.

En ese sentido se propone que al momento de ofrecer las tarjetas de crédito via telefónica o en sus agencias físicas, previo a su aceptación (contratación) también se registre en audio que se le informó sobre los riesgos que conlleva el no hacer un uso adecuado del producto que esta adquiriendo el usuario, se le informe que servicios adicionales tiene activos (operaciones por internet, disposiciones en efectivo, sobregiros), los canales de bloqueo, la protección de datos sensibles, el no entregar la tarjeta a terceras personas, el no ingresar a páginas no confiables y/o link, el cambio de la primera clave, todos los canales que tiene habilitado como compras por internet y su derecho de desactivarlos. Con ello, de manera preventiva se estaría protegiendo el interés económico del usuario de posibles riesgos a la que se ve expuesto que, si bien firmo haber tomado conocimiento de los riesgos, en la practica, no siempre el peruano lee lo que firma, y con ello, las entidades del sistema financiero estarían coadyuvando a brindar un servicio idóneo, y generando confianza en sus cientes al contratar sus productos y servicios.

El Reglamento de Tarjetas de Crédito y Débito ha señalado en su artículo 17° las siguientes medidas: (i) la entidad debe contar con un sistema de monitoreo que tendrá como finalidad detectar transacciones que se consideren no usuales, (ii) así mismo debe instaurar un procedimiento

para todas las advertencias que se generen en este sistema, (iii) debe identificar los patrones que puedan constituir un fraude, (iv) debe limitar el consumo en caso de alerta, tomando en cuenta que tiene la obligación de reducir las pérdidas por fraude, (v) debe requerir al titular el DNI cuando así se requiera o utilizar cualquier otra forma de identificación para validar la legitimidad del titular y (vi) cuando se efectué algún retiro o cualquier otra operación, debe exigirse la clave de acceso previamente consignada por el titular.

Entonces, si bien se estipula la obligación a las entidades de adoptar medidas de seguridad frente a operaciones inusuales, sin embargo, la forma en cómo se lleva a cabo este deber de monitoreo no se señala, más aún si el reglamento no estipula la forma en cómo se deben aplicar estas medidas de seguridad, especialmente el de monitoreo y deber de alerta por lo cual las aplica de acuerdo a sus propios criterios generando que no se actue de manera rápida para evitar la realización de más de una operación no reconocida.

Las denuncias administrativas por falta de adopción de medidas de seguridad en las tarjetas de crédito y débito en especial las que son objeto de estudio, las realizadas por internet, cuestionan por lo general múltiples operaciones realizadas, lo que lleva a evidenciar que la forma en cómo se lleva este monitoreo y aplicación de medidas de seguridad no resultan a la fecha eficientes para proteger los interes económicos del consumidor siendo necesario uniformizar criterios.

- Se propone que se refuerce el reglamento de tarjetas de crédito y débito

y se regule por parte de la SBS como las entidades bancarias y financieras deben de aplicar sus medidas de seguridad, es necesario la aplicación uniforme de sistemas de seguridad de estos últimos que impidan de manera total cualquier operación inusual; en tanto, ello es imposible hasta el momento, sin embargo si es exigible que la SBS regule cómo las entidades financieras y bancarias deben de aplicar el sistema de monitoreo y alerta de manera preventiva para identificar patrones de fraude de una forma más eficiente y que ante la minina sospecha de una operación inusual, se tomen las medidas correspondientes, evitando así que estas operaciones se concreten en perjuicio de los consumidores.

- Las medidas que se propone como criterio objetivo a aplicar por las entidades financieras y bancarias en cumplimiento al deber de monitoreo de operaciones es de bloquear de manera inmediata de manera preventiva la tarjeta cuando detecte una operación inusual bajo análisis de su área de fraude bajo criterios objetivos pero que estén regulados por la SBS de aplicación obligatoria para todos como por ejemplo; el numero de transacciones diarias que se realiza el cliente, montos mensuales que utiliza de sus fondos o línea disponible, el tipo de operación que efectua con frecuencia, el horario, etc, estandarización un único criterio.

  A la fecha si bien las entidades bancarias y financieras alertan en cumplimiento del reglamento de tarjetas de crédito y débito sobre la realización de las operaciones, ello aun sigue siendo insuficiente, toda vez que muchas veces proceden a bloquear la tarjeta de manera preventiva cuando ya se ha procesado varias operaciones en perjuicio del cliente,

ello en la medida que a la fecha no existe regulación de como aplicar el sistema de monitoreo siendo urgente que la SBS regule y de esta forma se uniformice el criterio de aplicación en salvaguarda de los intereses económicos del consumidor y en la generación de confianza sobre ellas dando de esta forma cumplimiento al articulo 65 de la Constitución Política del Perú: “El Estado defiende el interés de los consumidores y usuarios”.

CAPITULO V: DISCUSIÓN

Al examinar los sistemas de monitoreo de las instituciones bancarias y financieras, Balcazar (2017) concluyó que existe una capacidad limitada para detectar comportamientos inusuales de los tarjetahabientes de crédito o débito. Esta inadecuación puede causar un retraso en la identificación de cualquier problema relacionado con la actividad de la tarjeta. Al incorporar claves de bloqueo directo, actualizar los patrones de consumo de los clientes, implementar límites de consumo, tener confirmación de consumos posteriores a la operación a partir de ciertos montos e implementar controles más estrictos, la detección del fraude se realizará a tiempo o se evitará. El uso de tarjetas de débito debe reforzarse para apoyar estas medidas.

Se debe tener en cuenta, como destaca la investigación de Mora (2020) titulada "Resolución de transacciones no reconocidas con tarjetas de crédito o débito", que la identificación de patrones de consumo sospechosos se retrasa con frecuencia hasta que se han producido múltiples transacciones. Además, Mora sugiere que los bancos deben establecer sistemas de monitoreo efectivos para detectar tendencias fraudulentas y minimizar la frecuencia de dicho fraude en esta forma de transacción.

De esta manera se tiene que conforme Mora arriba a la conclusión que los sistemas de monitoreo de las entidades financieras no son efectivos pues retrazan su actuar, cuando ya se produjeron en muchos casos, un sinnúmeros de operaciones, recién proceden a efectuar e bloqueo preventivo por la generación de la alerta generando perjuicios económicos al usuario e incumpliendo su deber de idoneidad.

Cada cliente tiene un patrón de consumo habitual el cual va creando de acuerdo al historial de operaciones que realiza con una determinada tarjeta de crédito y/o débito. Como medidas de seguridad, es analizado por la entidad financiera a fin de determinar la inusualidad de las operaciones o su carácter de fraudulentas. Los resultados de la encuesta aplicada a los servidores públicos del INDECOPI de Ica, Arequipa y Tacna muestra las siguientes calificaciones respecto a la medida de seguridad de monitoreo de operaciones: para un 61% es regular, mientras que para el 23% son deficientes. El 10% opinó que es eficiente y el 6%, muy deficiente. Con ello queda se tiene que la percepción que tienen los servidores públicos sobre la idoneidad del monitoreo de operaciones que efectua las entidades fianancieras aun siguen siendo ineficaces, por lo cual se requiere ser reforzadas.

Los resultados de la presente investigación revelan que los servidores públicos del INDECOPI en Arequipa, Tacna e Ica, respecto a las reglas de seguridad definidas en el chip de las tarjetas de débito y crédito para realizar las operaciones financieras, el 48% lo calificó de regular, y el 29% de eficiente. Sólo el 23% lo consideró deficiente. Sobre el particular, las tarjetas deberán contar con un circuito integrado o chip que permita almacenar y procesar la información del usuario y sus operaciones, cumpliendo estándares internacionales de interoperabilidad para el uso y verificación de las tarjetas, así como para la autenticación de pagos; para lo cual deberá cumplirse como mínimo con los requisitos de seguridad establecidos en el estándar EMV, emitido por EMVCo.

La investigación de Balcazar (2017) destaca la importancia de las claves secretas para garantizar la seguridad de las tarjetas de crédito y débito. Estas

claves brindan acceso completo y permiten el uso de la tarjeta. Cuando el Indecopi busca registros de transacciones del supuesto “titular”, los informes correspondientes de Tándem y Diarios son entregados por el banco o entidad financiera. Sin embargo, dicha información indica únicamente la conformidad con el procedimiento estándar debido a la entrada correcta de la clave secreta. En consecuencia, ya no es suficiente determinar si una operación es auténtica o no autorizada.

Las operaciones por internet tienen ventaja frente a las operaciones realizadas de manera tradicional. Los resultados de la investigación señalan que el 32% de los usuarios encuestados considera a la accesibilidad como principal ventaja sobre las operaciones por internet. Así mismo, el 25% considera a la rapidez como ventaja sobre las operaciones por internet.

Los resultados de la presente investigación señalan que el 90% de los usuarios tiene conocimiento que puede realizar operaciones por internet con su tarjeta de crédito y/o débito, y el 10% no tiene conocimiento que puede realizar operaciones por internet con su tarjeta de crédito y/o débito.

Bances (2021) concluye que la educación financiera se relaciona con sus capacidades financieras adquiridas, como un aspecto clave de la administración financiera. Los resultados determinaron que existe una relación significativa media (Tb=, 413) entre educación financiera y capacidades financieras en los colaboradores de entidades educativas, siendo evidente que a mayor acceso y participación en educación financiera, mayores serán las capacidades financieras manifiestas en los individuos. Por tanto, en el ámbito del manejo de finanzas personales, es importante fomentar el desarrollo de la educación

financiera y se considera pertinente seguir potenciando estrategias para mejorar la administración de los recursos en los colaboradores de las entidades educativas, al estar relacionada con las capacidades financieras manifestadas en el uso y manejo de herramientas financieras; de allí que, es oportuno la construcción de escenarios de formación y educación financiera en los colaboradores para mejorar las capacidades financieras.

CONCLUSIONES

- Los mecanismos de seguridad se relacionan con las operaciones por internet según las denuncias ingresadas en los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021. El interés de las operaciones por internet está relacionado con los mecanismos de seguridad respecto al uso de tarjetas de crédito y débito. Al respecto con la presente investigación se ha demostrado que existe una relación entre los mecanismos de seguridad en referencia al interés de efectuar operaciones por internet respecto de los usuarios, toda vez que si bien la SBS regula las medidas a adoptarse, estas a la fecha vienen siendo ineficaces, debiendo de fortalecerse respecto al como debe de aplicarlas las entidades financieras.

- Falta un reforzamiento del reglamento de tarjetas de crédito y débito y se regule por parte de la SBS como las entidades bancarias y financieras deben de aplicar sus medidas de seguridad, es necesario la aplicación uniforme de sistemas de seguridad de estos últimos que impidan de manera total cualquier operación inusual; en tanto, ello es imposible hasta el momento, sin embargo si es exigible que la SBS regule cómo las entidades financieras y bancarias deben de aplicar el sistema de monitoreo y alerta de manera preventiva para identificar patrones de fraude de una forma más eficiente y que ante la minina sospecha de una operación inusual, se tomen las medidas correspondientes, evitando así que estas operaciones se concreten en perjuicio de los consumidores.

- A la fecha si bien las entidades bancarias y financieras alertan en cumplimiento del reglamento de tarjetas de crédito y débito sobre la realización de las operaciones, ello aun sigue siendo insuficiente, toda vez que muchas veces proceden a bloquear la tarjeta de manera preventiva cuando ya se ha procesado varias operaciones en perjuicio del cliente, ello en la medida que a la fecha no existe regulación de como aplicar el sistema de monitoreo siendo urgente que la SBS regule y de esta forma se uniformice el criterio de aplicación en salvaguarda de los intereses económicos del consumidor y en la generación de confianza sobre ellas dando de esta forma cumplimiento al articulo 65 de la Constitución Política del Perú: “El Estado defiende el interés de los consumidores y usuarios”.

- Las medidas de seguridad incorporadas en las tarjetas se relacionan con las operaciones por internet según las denuncias ingresadas en los ORPS del INDECOPI de Ica, Arequipa y Tacna, 2021. El interés de las operaciones por internet está relacionado con las medidas de seguridad incorporadas en las tarjetas de débito y crédito, por lo cual es necesario que se priorice las tarjetas de crédito y débito digitales que ofrecen el CVV dinámico cuya función es proteger sus datos y evitar que sean usados de una segunda vez. Asimismo, se propone que la entidad financiera emisora le expida una tarjeta que no tenga los números al frente para mantener oculta la información sensible a simple vista.

- La poca educación financiera es otro de los factores que influye, si bien en los contratos adhesivos la entidad financiera consigna los derechos y

obligaciones, canales de atención, que hacer en caso de perdida, robo, etc de la tarjeta, o mantenerla en custodia, el derecho de activar y desactivar notificaciones de realización de operaciones, servicios adicionales como sobregiros, compras en el exterior, compras por internet, disposición en efectivo; sin embargo, no es menos cierto que la tendencia es no leer lo que se firma, y en consecuencia no saber que el solo hecho de haber contratado una tarjeta de crédito trae consigo además de beneficios, peligros a los cuales me veo expuesto, si no cumplo con las condiciones de seguridad pactadas.

RECOMENDACIONES

- El Indecopi debe de recomendar a las entidad financieras efectuar una capacitación de educación financiera a sus clientes, a través de su personal encargado de expedir tarjetas de crédito y débito como a las que terceriza dicho servicio a fin de que estos informen de manera previa a la contratación del producto financiero no solo de manera escrita en el contrato sino también de manera verbal, teniendo en cuenta que el peruano no tiene como política leer lo que firma, una explicación detallada de los riesgos que implica no custodiar de manera adecuada su tarjeta de crédito y debito.

- Se recomienda que la SBS regule cómo debe aplicar las entidades financieras el sistema de monitoreo o deber de alerta en las operaciones inusuales, estableciendo un criterio general para todas, toda vez que las medidas de seguridad implementadas por las entidades financieras ante la detección de operaciones inusuales reglamentada por la SBS no vienen siendo aplicadas de forma efectiva para el resguardo de los intereses económicos del consumidor, en tanto no hay una regulación y las entidades financieras utilizan criterios propios.

- Se recomienda que las entidades bancarias y financieras prioricen las tarjetas de crédito y débito digitales que ofrecen el CVV dinámico cuya función es proteger sus datos y evitar que sean usados de una segunda vez. Asimismo, se recomienda que la entidad financiera emisora expida a sus clientes una tarjeta que no tenga los números al frente para mantener oculta la información sensible a simple vista.

FUENTES DE INFORMACIÓN

Alva, F. (11 de 08 de 2021). *https://lpderecho.pe/medidas-seguridad-consumos-no-reconocidos-tarjetas-credito-debito/*. Obtenido de lpderecho.pe: https://lpderecho.pe/medidas-seguridad-consumos-no-reconocidos-tarjetas-credito-debito/

Arequipa, C. (06 de 2020). *https://www.cajaarequipa.pe/documents/preguntas-frecuentes-internet-cajaarequipa-24-03-2017.pdf*. Obtenido de http://www.cajaarequipa.pe/: https://www.cajaarequipa.pe/documents/preguntas-frecuentes-internet-cajaarequipa-24-03-2017.pdf

Bahillo, M. E.; Pérez, M. C. (2017). *Operaciones auxiliares de gestión de tesorería.* Ediciones Paraninfo. Obtenido de https://books.google.com.pe/books?id=_WkpDwAAQBAJ&printsec=frontcover&dq=Operaciones+auxiliares+de+gesti%C3%B3n+de+tesorer%C3%ADa&hl=es419&sa=X&ved=0ahUKEwj8rcTf_eLcAhWNT98KHS1cCQYQ6wEIKDAA#v=onepage&q=Operaciones%20auxiliares%20de%20gesti%C3%B3n%20de%20

Balcazar, W. (2017). *Universidad Privada Antenor Orrego]*. Obtenido de http://repositorio.upao.edu.pe/handle/upaorep/3314: http://repositorio.upao.edu.pe/handle/upaorep/3314

Balcazar, W. Y. (2017). *Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito.* Universidad Privada Antenor Orrego - UPAO, Trujillo. repositorio.upao.edu.pe. Obtenido de http://repositorio.upao.edu.pe/handle/upaorep/3314

BeharD., D. (2008). *METODOLOGÍA DE LA INVESTIGACIÓN.* Shalom.

cajaarequipa.pe. (24 de 03 de 2017). *https://www.cajaarequipa.pe/documents/preguntas-frecuentes-internet-cajaarequipa-24-03-2017.pdf*. Obtenido de https://www.cajaarequipa.pe/documents/preguntas-frecuentes-internet-cajaarequipa-24-03-2017.pdf: https://www.cajaarequipa.pe/documents/preguntas-frecuentes-internet-cajaarequipa-24-03-2017.pdf

Cuervo, J. (28 de 04 de 2021). *https://www.informatica-juridica.com/author/josecuervo/page/2/*. (J. Cuervo, Editor) Recuperado el 20 de 06 de 2022, de Informática Jurídica: https://www.informatica-juridica.com/author/josecuervo/page/2/

Cusacani, Yudith Karina; Ttito, Jeni. (2019). *Influencia de la cultura financiera en el uso de la tarjeta de débito y crédito en los clientes del Banco Continental - agencia Miraflores - Arequipa, 2018*. Obtenido de http://repositorio.upao.edu.pe/handle/upaorep/3314

Escoto, R. (2007). Banca Comercial. (U. e. distancia, Ed.) 108. Obtenido de https://books.google.com.pe/books?id=oDIBV4vO54IC&pg=PA108&dq=La+tarjeta+de+d%C3%A9bito+es+un+pl%C3%A1stico+con+banda+magn%C3%A9tica+que+permite+utilizar+los+fondos+disponibles+en+una+cuenta+de+ahorros+para+realizar+compras+en+puntos+de+ventas+o+retirar+y

Flores, Emilio ; Pilco, Mesías Heriberto ; Haro, Pablo Patricio. (2015). El uso de las tarjetas de crédito y débito en la sociedad actual. *Revista Caribeña de Ciencias Sociales*. Obtenido de

https://www.eumed.net/rev/caribe/2015/08/tarjetas-credito.html

Gómez, G. G. (21 de 05 de 21). *Ciberseguridad: ¿Cuáles son los robos y las estafas más comunes en el mundo digital?* Obtenido de esan.edu.pe/conexion-esan/ciberseguridad-cuales-son-los-robos-y-las-estafas-mas-comunes-en-el-mundo-digital: esan.edu.pe/conexion-esan/ciberseguridad-cuales-son-los-robos-y-las-estafas-mas-comunes-en-el-mundo-digital

Guarnizo, Paula Natalia ; Segura, María Camila. (2018). Responsabilidad de las entidades financieras en eventos de fraudes electrónicos. *Revista NUEVA ÉPOCA de la Universidad Libre*. Obtenido de https://revistas.unilibre.edu.co/index.php/nueva_epoca/article/view/3630

Hernández, R., Fernandez, C., & Baptista, M. (2014). *Metodología de la* (Vol. Vol. 6ta Edicion). México.

Hernández, R., Fernandez, C., & Baptista, M. (2014). *Metodología de la Investigación.* México: McGRAW-HILL/INTERAMERICANA.

INDECOPI. (2010). Glosario de áreas del Reporte de Estadísticas Institucionales. *INDECOPI*, 2. Obtenido de https://www.consumidor.gob.pe/documents/20182/174845/Rep_Men_Glosario/a2bd8f91-1987-4eff-a912-a68a6ac9b0fb#:~:text=El%20Servicio%20de%20Atenci%C3%B3n%20al,la%20Propiedad%20Intelectual%20(Indecopi).

INDECOPI. (2010). *indecopi.gob.pe*. Obtenido de indecopi.gob.pe: https://www.indecopi.gob.pe/documents/20182/174845/Glosario.pdf/ed79a336-467b-40ae-9073-f2af715f1ab1

Linares , L. d. (2020). *El deber de idoneidad de las entidades bancarias de la*

región La Libertad en el fraude electrónico con tarjetas de crédito y débito. Universidad Privada del Norte, Lima. Lima: Universidad Privada del Norte. Obtenido de https://hdl.handle.net/11537/25849

LpDerecho. (21 de 08 de 2021). *https://lpderecho.pe/medidas-seguridad-consumos-no-reconocidos-tarjetas-credito-debito/https://lpderecho.pe/medidas-seguridad-consumos-no-reconocidos-tarjetas-credito-debito/*. Obtenido de https://lpderecho.pe/medidas-seguridad-consumos-no-reconocidos-tarjetas-credito-debito/: https://lpderecho.pe/medidas-seguridad-consumos-no-reconocidos-tarjetas-credito-debito/

Meza, P. (09 de 2012). *http://repositorio.upao.edu.pe/handle/upaorep/3314*. Obtenido de http://repositorio.upao.edu.pe/handle/upaorep/3314

Meza, P. V. (2012). *El estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación.* Pontificia Universidad Católica del Perú, Lima. Lima: Pontificia Universidad Católica del Perú. Obtenido de http://hdl.handle.net/20.500.12404/1668

Molano, Yuly Alexandra; Correa, Yamir. (2016). *Predicción del fraude con tarjetas para una entidad financiera a través del modelo Arimax.* Fundación Universitaria Los Libertadores, Bogotá D.C. Obtenido de http://hdl.handle.net/11371/760

Mora, C. M. (2020). *Criterios para resolver casos de operaciones no reconocidas efectuadas mediante el uso de tarjetas de crédito o débito.* Pontificia Universidad Católica del Perú. Facultad de Derecho, Lima. Lima: PUCP.

Paz, A. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. Una mirada a la

jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia. *Revista de Derecho Privado de la Universidad Externado de Colombia*. Obtenido de https://revistas.uexternado.edu.co/index.php/derpri/article/view/5536

Perú, S. d. (2013). *Superintendencia de Banca y Seguros del Perú*. Obtenido de Resolución SBS N° 6523-2013: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20 500.12404/19164/MORA_CABRERA_CRISTIAN_MAURO%20%281%29.pdf?sequence=1&isAllowed=y

Pierino, José; Antonio, Oscar. (2021). *Manual de Derecho del consumidor aplicado a los servicios bancarios.* Lima, Perú: Palestra Editores. Obtenido de https://books.google.com.pe/books?id=148pEAAAQBAJ&pg=PT106&lpg=PT106&dq=%22Se+refiere+al+tipo+de+operaciones+que+usualmente+realiza+cada+usuario+con+sus+tarjetas,+considerando+diversos+factores,+como+por+ejemplo+el+pa%C3%ADs+de+consumo,+tipos+de+comercio,

repositorio.unsa.edu.pe. (s.f.). *http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/9098/BScumayk%26tttoje.pdf?isAllowed=y&sequence=1*. Obtenido de http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/9098/BScumayk%26tttoje.pdf?isAllowed=y&sequence=1: http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/9098/BScumayk%26tttoje.pdf?isAllowed=y&sequence=1

Silvestre, J. K. (2021). *La aplicación de medidas de seguridad para casos de*

operaciones inusuales en tarjetas de crédito y débito en materia de protección al consumidor. Pontificia Universidad Católica del Perú, Lima. Lima: Pontificia Universidad Católica del Perú. Obtenido de http://hdl.handle.net/20.500.12404/21054

UNSA. (2019). *http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/9098/BScumayk%26tttoje.pdf?isAllowed=y&sequence=1*. Obtenido de http://repositorio.unsa.edu.pe/: http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/9098/BScumayk%26tttoje.pdf?isAllowed=y&sequence=1

ANEXOS

Anexo 1: Reglamento de Tarjetas de Crédito y Débito y modificatorias.

NORMA QUE MODIFICA	ACCION	NUMERO	TIPO	ESTADO ACUAL	VERSION ACTUAL	FECHA DE EJECUCION DE LA ACCION
Resolución de la Superintendencia de Banca y Seguros N° 6523-2013 (v7.0)	Derogada a	Circular B-1848-1990, M-194-90, CM-063-90 (v1.0)	Circular	Derogada	V1.0	01/04/2014
Resolución de la Superintendencia de Banca y Seguros N° 6523-2013 (v2.0)	Modificada por	Resolución de la Superintendencia de Banca y Seguros N° 6617-2016 (v1.0)	Resolución	Vigente	V1.0	26/12/2016
Resolución de la Superintendencia de Banca y Seguros N° 6523-2013 (v1.0)	Modificada por	Resolución de la Superintendencia de Banca y Seguros N° 652-2016 (v1.0)	Resolución	Vigente	V1.0	10/02/2016
Resolución de la Superintendencia de Banca y Seguros N° 6523-2013 (v3.0)	Modificada por	Resolución de la Superintendencia de Banca y Seguros N° 3274-2017 (v1.0)	Resolución	Vigente	V6.0	01/11/2017
Resolución de la Superintendencia de Banca y Seguros N° 6523-2013 (v5.0)	Modificada por	Resolución de la Superintendencia de Banca y Seguros N° 5570-2019 (v1.0)	Resolución	Vigente	V3.0	29/11/2019
Resolución de la Superintendencia de Banca y Seguros N° 6523-2013 (v6.0)	Modificada por	Resolución de la Superintendencia de Banca y Seguros N° 5570-2019 (v3.0)	Resolución	Vigente	V3.0	01/07/2021

Fuente: Elaboración propia

Anexo 2: Cuestionario 1

El cuestionario busca determinar el grado de eficiencia con respecto a las medidas de seguridad implementadas para el uso de tarjetas de crédito y débito en operaciones por internet.

El cuestionario se aplicará a los servidores públicos trabajadores de las Oficinas Regionales del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual de Ica, Arequipa y Tacna.

Instrucciones: Por favor, a continuación indique su grado de eficiencia con los siguientes enunciados, en una escala del 1 al 5, según los valores siguientes:

1	2	3	4	5
Muy deficiente	Deficiente	Regular	Eficiente	Muy eficiente

Enunciados	1	2	3	4	5
Variable independiente: Medidas de seguridad					
Dimensión: Medidas de seguridad incorporadas en las tarjetas					
1. ¿Qué opina sobre las reglas de seguridad definidas en el chip de las tarjetas de débito y crédito?					
2. ¿Qué tan eficiente le parecen los procedimientos criptográficos sobre datos críticos?					
3. ¿Qué tan eficiente es usar método de autenticación de datos?					
4. ¿Qué tan eficiente son las instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea?					
Dimensión: Medidas de seguridad respecto a los usuarios					
5. ¿Qué tan eficiente es la entrega de tarjeta a titular?					
6. ¿Qué tan eficiente es el cambio de primera clave o número secreto de la tarjeta?					
7. ¿Qué tan eficiente resulta el servicio de notificaciones mediante mensajes de texto, a un correo electrónico y/o un teléfono móvil, entre otros mecanismos?					
8. ¿Qué tan eficiente resulta comunicar a la empresa que realizarán operaciones con su tarjeta desde el extranjero?					
Dimensión: Medidas de seguridad respecto al monitoreo y realización de operaciones					
9. ¿Qué tan eficiente son los sistemas de monitoreo de operaciones que detectan operaciones que no corresponden al comportamiento habitual de consumo del usuario?					
10. ¿Qué opina sobre la identificación de patrones de fraude?					
11. ¿Qué tan eficiente son los controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude?					
12. ¿Qué tan eficiente resulta la presentación de un documento oficial de identidad?					
Variable dependiente: Operaciones por internet					
Dimensión: sistemas informaticos que incluye software					
13. ¿Qué opina sobre la configuración de cortafuegos o firewalls, enrutadores y equipos similares?					

14. ¿Qué tan eficiente es el software y programas antivirus en computadores y servidores?					
15. ¿Califique sobre los sistemas informáticos y aplicaciones seguras para las operaciones por internet?					
Dimensión: Política de protección de la información del tarjetahabiente frente a la vulnerabilidad de la realización de operaciones por internet					
16. ¿Qué tan eficientes son las políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados provistos por los proveedores de servicios de tecnología?					
17. ¿Qué tan eficientes son las políticas que restrinjan el acceso a los datos de los usuarios solo al personal autorizado, reduciéndolo al estrictamente necesario?					
18. ¿Qué tan eficientes son las políticas de asignación de un identificador único a cada persona que acceda a través de software a los datos de los usuarios?					
19. ¿Califique los controles de acceso físico para proteger los datos de los usuarios?					
20. ¿Califique el registro y monitoreo todos los accesos a los recursos de red y a los datos de los usuarios?					
Dimensión: relacionado a eficiencia de las medidas de seguridad					
21. ¿Qué tan eficiente es el análisis de vulnerabilidades periódicos a la red interna y pruebas de penetración externas e internas?					
22. ¿Qué tan eficiente es el plan de respuesta a eventos de violación de seguridad?					
23. ¿Qué tan eficientes son los procedimientos de aceptación de las operaciones, incluyendo entre otros la verificación de la validez de la tarjeta, la identidad del usuario, y la firma en caso de ser aplicable?					
24. ¿Qué tan eficiente es no guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta?					

ANEXO 3: Cuestionario 2

El cuestionario busca determinar el grado de eficiencia con respecto a las medidas de seguridad implementadas para el uso de tarjetas de crédito y débito en operaciones por internet.

El cuestionario se aplicó a usuario que utilizan las tarjetas de crédito y debito en el sistema financiero bancario.

Instrucciones: Por favor, a continuación, responda conforme a los siguientes enunciados.

1. ¿Tiene conocimiento que puede realizar operaciones en internet con su tarjeta de crédito y/o débito?
   A. Si
   B. No
2. ¿Ha realizado alguna vez operaciones por internet?
   A. Si
   B. No
3. ¿Qué tipo de operaciones ha realizado en el último año a través de la Banca Móvil o mediante la Banca por Internet?
   A. Realizar compras en línea
   B. Realizar pagos de servicios
   C. Transferencias entre cuentas y a terceros
   D. Ninguna de las anteriores

E. Todas las anteriores

4. ¿Cuál de las siguientes aplicaciones ha utilizado para realizar operaciones en internet?

   A. Aplicación móvil

   B. Sitio Web

   C. Otros

5. ¿Ha tenido algún problema con el uso fraudulento de su tarjeta de crédito y/o débito en el último año?

   A. Si

   B. No

6. ¿Cree que siempre se debería pedir la identificación de la identidad del tarjetahabiente para realizar una operación con tarjeta de crédito y/o débito?

   A. Si

   B. No

7. Su experiencia al realizar operaciones por internet fue

   A. Muy satisfactorio

   B. Satisfactorio

   C. Indiferente

   D. Insatisfecho

   E. Muy insatisfecho

8. A continuación, le presentamos las ventajas sobre las operaciones por internet. Por favor, señale, en orden de prioridad, las cinco más importante para usted.

   A. Facilidad de uso
   B. Comodidad
   C. Seguro
   D. Accesibilidad
   E. Rapidez
   F. Eficiencia
   G. Asistencia en la compra
   H. Otros

9. ¿Cuáles de los aspectos le impedirían realizar operaciones por internet?

   Por favor, señale, en orden de prioridad las cinco más importantes para usted.

   A. Temor a la estafa
   B. No cuenta con medios necesarios
   C. Dificultad en el uso
   D. Desconfianza de proporcionar datos personales
   E. No le interesa
   F. Prefiero ver lo que compro
   G. Ningunas de las anteriores
   H. Otros

Informes de validación del instrumento

INFORME DE JUICIO DE EXPERTO SOBRE INSTRUMENTO DE INVESTIGACIÓN
CUESTIONARIO A

I. DATOS GENERALES

- Título de la investigación: Los mecanismos de seguridad en las operaciones bancarias por internet en los órganos resolutivos de procedimientos sumarísimos (ORPS) de Ica, Arequipa y Tacna 2021.
- Apellidos y nombres del experto: Carlos Guillermo Moises Medina Quichca
- Grado académico: Abogado
- Institución en la que trabaja el experto: Indecopi
- Cargo que desempeña: Especialista en Derecho
- Instrumento motivo de evaluación: Cuestionario
- Autor del instrumento: Maritza Elizabeth Ochoa Quispe

II. ASPECTOS DE VALIDACIÓN:

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (2) BUENO (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están formulados con lenguaje apropiado, es decir libre de ambigüedades.					X
OBJETIVIDAD	Los ítems del instrumento permitirán medir la variable en todas sus dimensiones e indicadores en sus aspectos conceptuales y operacionales.					X
ACTUALIDAD	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal.				X	
ORGANIZACIÓN	Los ítems del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual relacionada con las variables en todas dimensiones e indicadores, de manera que permitan hacer abstracciones e inferencia en función a los problemas y objetivos.					X
SUFICIENCIA	Los ítems del instrumento expresan suficiencia en cantidad y calidad.					X
INTENCIONALIDAD	Los ítems del instrumento evidencian ser adecuados para el examen de contenido y mensuración de las evidencias inherentes.				X	
CONSISTENCIA	La información que se obtendrá mediante los ítems permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan coherencia entre la variable, dimensiones e indicadores.					X
METODOLOGIA	Los procedimientos insertados en el instrumento responden al propósito de la investigación.					X
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
	SUBTOTAL				8	40
	TOTAL	48				

III. OPINIÓN DE APLICACIÓN: Es válido para su aplicación.
IV. PROMEDIO DE VALIDACIÓN: 4.8

Ica, 19 setiembre del 2022

Firma del Experto
DNI N° 72324194

INFORME DE JUICIO DE EXPERTO SOBRE INSTRUMENTO DE INVESTIGACIÓN
CUESTIONARIO B

I. DATOS GENERALES

- Título de la Investigación: Los mecanismos de seguridad en las operaciones bancarias por internet en los órganos resolutivos de procedimientos sumarísimos (ORPS) de Ica, Arequipa y Tacna 2021.
- Apellidos y nombres del experto: Carlos Guillermo Moises Medina Quichca
- Grado académico: Abogado
- Institución en la que trabaja el experto: Indecopi
- Cargo que desempeña: Especialista en Derecho
- Instrumento motivo de evaluación: Cuestionario
- Autor del instrumento: Maritza Elizabeth Ochoa Quispe

II. ASPECTOS DE VALIDACIÓN:

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (2) BUENO (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están formulados con lenguaje apropiado, es decir libre de ambigüedades.					X
OBJETIVIDAD	Los ítems del instrumento permitirán medir la variable en todas sus dimensiones e indicadores en sus aspectos conceptuales y operacionales.					X
ACTUALIDAD	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal.				X	
ORGANIZACIÓN	Los ítems del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual relacionada con las variables en todas dimensiones e indicadores, de manera que permiten hacer abstracciones e inferencia en función a los problemas y objetivos.					X
SUFICIENCIA	Los ítems del instrumento expresan suficiencia en cantidad y calidad.					X
INTENCIONALIDAD	Los ítems del instrumento evidencian ser adecuados para el examen de contenido y mensuración de las evidencias inherentes.				X	
CONSISTENCIA	La información que se obtendrá mediante los ítems permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan coherencia entre la variable, dimensiones e indicadores.					X
METODOLOGIA	Los procedimientos insertados en el instrumento responden al propósito de la investigación.					X
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
	SUBTOTAL				8	40
	TOTAL	48				

III. OPINIÓN DE APLICACIÓN: Es válido para su aplicación.
IV. PROMEDIO DE VALIDACIÓN: 4.8

Ica, 19 setiembre del 2022

Firma del Experto
DNI N° 72324194

INFORME DE JUICIO DE EXPERTO SOBRE INSTRUMENTO DE INVESTIGACIÓN
CUESTIONARIO A

I. DATOS GENERALES

- Título de la Investigación: Los mecanismos de seguridad en las operaciones bancarias por internet en los órganos resolutivos de procedimientos sumarísimos (ORPS) de Ica, Arequipa y Tacna 2021.
- Apellidos y nombres del experto: Carlos Alberto Huarcaya García
- Grado académico: Abogado
- Institución en la que trabaja el experto: Indecopi
- Cargo que desempeña: Especialista Legal
- Instrumento motivo de evaluación: Cuestionario
- Autor del instrumento: Maritza Elizabeth Ochoa Quispe

II. ASPECTOS DE VALIDACIÓN:

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENO (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están formulados con lenguaje apropiado, es decir libre de ambigüedades.					X
OBJETIVIDAD	Los ítems del instrumento permitirán medir la variable en todas sus dimensiones e indicadores en sus aspectos conceptuales y operacionales.					X
ACTUALIDAD	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal.				X	
ORGANIZACIÓN	Los ítems del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual relacionada con las variables en todas dimensiones e indicadores, de manera que permitan hacer abstracciones e inferencia en función a los problemas y objetivos.					X
SUFICIENCIA	Los ítems del instrumento expresan suficiencia en cantidad y calidad.					X
INTENCIONALIDAD	Los ítems del instrumento evidencian ser adecuados para el examen de contenido y mensuración de las evidencias inherentes.				X	
CONSISTENCIA	La información que se obtendrá mediante los ítems permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan coherencia entre la variable, dimensiones e indicadores.					X
METODOLOGIA	Los procedimientos insertados en el instrumento responden al propósito de la investigación.					X
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
	SUBTOTAL				8	40
	TOTAL	48				

III. OPINIÓN DE APLICACIÓN: Es válido para su aplicación.
IV. PROMEDIO DE VALIDACIÓN: 4.8

Ica, setiembre del 2022

Firma del Experto
DNI N°42074816

INFORME DE JUICIO DE EXPERTO SOBRE INSTRUMENTO DE INVESTIGACIÓN
CUESTIONARIO B

I. DATOS GENERALES

- Título de la Investigación: Los mecanismos de seguridad en las operaciones bancarias por internet en los órganos resolutivos de procedimientos sumarísimos (ORPS) de Ica, Arequipa y Tacna 2021.
- Apellidos y nombres del experto: Carlos Alberto Huarcaya García
- Grado académico: Abogado
- Institución en la que trabaja el experto: Indecopi
- Cargo que desempeña: Especialista Legal
- Instrumento motivo de evaluación: Cuestionario
- Autor del instrumento: Maritza Elizabeth Ochoa Quispe

II. ASPECTOS DE VALIDACIÓN:

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (2) BUENO (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están formulados con lenguaje apropiado, es decir libre de ambigüedades.					X
OBJETIVIDAD	Los ítems del instrumento permitirán medir la variable en todas sus dimensiones e indicadores en sus aspectos conceptuales y operacionales.					X
ACTUALIDAD	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal.				X	
ORGANIZACIÓN	Los ítems del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual relacionada con las variables en todas dimensiones e indicadores, de manera que permitan hacer abstracciones e inferencia en función a los problemas y objetivos.					X
SUFICIENCIA	Los ítems del instrumento expresan suficiencia en cantidad y calidad.					X
INTENCIONALIDAD	Los ítems del instrumento evidencian ser adecuados para el examen de contenido y mensuración de las evidencias inherentes.				X	
CONSISTENCIA	La información que se obtendrá mediante los ítems permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan coherencia entre la variable, dimensiones e indicadores.					X
METODOLOGIA	Los procedimientos insertados en el instrumento responden al propósito de la investigación.					X
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
	SUBTOTAL				8	40
	TOTAL	48				

III. OPINIÓN DE APLICACIÓN: Es válido para su aplicación.
IV. PROMEDIO DE VALIDACIÓN: 4.8

Ica, setiembre del 2022

Firma del Experto
DNI N° 42074816

INFORME DE JUICIO DE EXPERTO SOBRE INSTRUMENTO DE INVESTIGACIÓN
CUESTIONARIO A

I. DATOS GENERALES

- Título de la Investigación: Los mecanismos de seguridad en las operaciones bancarias por internet en los órganos resolutivos de procedimientos sumarísimos (ORPS) de Ica, Arequipa y Tacna 2021.
- Apellidos y nombres del experto: Antony Aquilino De La Cruz Martinez
- Grado académico: Abogado
- Institución en la que trabaja el experto: Indecopi
- Cargo que desempeña: Especialista en Derecho
- Instrumento motivo de evaluación: Cuestionario
- Autor del instrumento: Maritza Elizabeth Ochoa Quispe

II. ASPECTOS DE VALIDACIÓN:

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (2) BUENO (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están formulados con lenguaje apropiado, es decir libre de ambigüedades.					X
OBJETIVIDAD	Los ítems del instrumento permitirán medir la variable en todas sus dimensiones e indicadores en sus aspectos conceptuales y operacionales.				X	
ACTUALIDAD	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal.					X
ORGANIZACIÓN	Los ítems del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual relacionada con las variables en todas dimensiones e indicadores, de manera que permiten hacer abstracciones e inferencia en función a los problemas y objetivos.					X
SUFICIENCIA	Los ítems del instrumento expresan suficiencia en cantidad y calidad.					X
INTENCIONALIDAD	Los ítems del instrumento evidencian ser adecuados para el examen de contenido y mensuración de las evidencias inherentes.					X
CONSISTENCIA	La información que se obtendrá mediante los ítems permitirá analizar, describir y explicar la realidad motivo de la investigación.				X	
COHERENCIA	Los ítems del instrumento expresan coherencia entre la variable, dimensiones e indicadores.					X
METODOLOGÍA	Los procedimientos insertados en el instrumento responden al propósito de la investigación.					X
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
	SUBTOTAL				8	40
	TOTAL			48		

III. OPINIÓN DE APLICACIÓN: Es válido para su aplicación.
IV. PROMEDIO DE VALIDACIÓN: 4.8

Ica, 20 setiembre del 2022

Firma del Experto
DNI N° 45892215

INFORME DE JUICIO DE EXPERTO SOBRE INSTRUMENTO DE INVESTIGACIÓN
CUESTIONARIO B

I. DATOS GENERALES

- Título de la investigación: Los mecanismos de seguridad en las operaciones bancarias por internet en los órganos resolutivos de procedimientos sumarísimos (ORPS) de Ica, Arequipa y Tacna 2021.
- Apellidos y nombres del experto: Antony Aquilino De La Cruz Martinez
- Grado académico: Abogado
- Institución en la que trabaja el experto: Indecopi
- Cargo que desempeña: Especialista en Derecho
- Instrumento motivo de evaluación: Cuestionario
- Autor del instrumento: Maritza Elizabeth Ochoa Quispe

II. ASPECTOS DE VALIDACIÓN:

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (2) BUENO (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están formulados con lenguaje apropiado, es decir libre de ambigüedades.					X
OBJETIVIDAD	Los ítems del instrumento permitirán medir la variable en todas sus dimensiones e indicadores en sus aspectos conceptuales y operacionales.				X	
ACTUALIDAD	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal.					X
ORGANIZACIÓN	Los ítems del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual relacionada con las variables en todas dimensiones e indicadores, de manera que permitan hacer abstracciones e inferencia en función a los problemas y objetivos.					X
SUFICIENCIA	Los ítems del instrumento expresan suficiencia en cantidad y calidad.				X	
INTENCIONALIDAD	Los ítems del instrumento evidencian ser adecuados para el examen de contenido y mensuración de las evidencias inherentes.					X
CONSISTENCIA	La información que se obtendrá mediante los ítems permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan coherencia entre la variable, dimensiones e indicadores.					X
METODOLOGÍA	Los procedimientos insertados en el instrumento responden al propósito de la investigación.					X
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
	SUBTOTAL				8	40
	TOTAL	48				

III. OPINIÓN DE APLICACIÓN: Es válido para su aplicación.
IV. PROMEDIO DE VALIDACIÓN: 4.8

Ica, 20 de setiembre del 2022

Firma del Experto
DNI N° 45892215