



**FACULTAD DE POSTGRADO  
TRABAJO FINAL DE GRADUACIÓN**

**EVOLUCIÓN DE LAS TARJETAS DE CRÉDITO COMO MEDIO  
DE PAGO SEGURO**

**SUSTENTADO POR:**

**RUTH MARIA VÁSQUEZ PORTILLO**

**PREVIA INVESTIDURA AL TÍTULO DE**

**MÁSTER EN  
DIRECCION EMPRESARIAL**

**TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.**

**SEPTIEMBRE, 2021**

**UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA**

**UNITEC**

**FACULTAD DE POSTGRADO**

**AUTORIDADES UNIVERSITARIAS**

**RECTOR**

**MARLON ANTONIO BREVÉ REYES**

**SECRETARIO GENERAL**

**ROGER MARTÍNEZ MIRALDA**

**VICERRECTORA ACADÉMICA**

**DESIREE TEJADA CALVO**

**DIRECTORA NACIONAL DE POSTGRADO**

**ANA DEL CARMEN RETTALLY**

**EVOLUCIÓN DE LAS TARJETAS DE CRÉDITO COMO  
MEDIO DE PAGO SEGURO**

**TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS  
REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE  
MÁSTER EN**

**DIRECCIÓN EMPRESARIAL**

**ASESOR**

**ALBERTINA NAVARRO**

**COMITÉ EVALUADOR:**

**JOSE MARCELO FLORES  
JORGE CENTENO**

# **DERECHOS DE AUTOR**

© Copyright 2021  
Ruth María Vásquez Portillo

Todos los derechos son reservados.

**AUTORIZACIÓN DEL AUTOR(ES) PARA LA CONSULTA,  
REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN  
ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS DE POSTGRADO**

Señores

**CENTRO DE RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN (CRAI)  
UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA (UNITEC)**

Estimados Señores:

Yo, Ruth María Vásquez Portillo, de Tegucigalpa, (o San Pedro Sula, o La Ceiba) autor del trabajo de postgrado titulado: EVOLUCIÓN DE LAS TARJETAS DE CRÉDITO COMO MEDIO DE PAGO SEGURO, presentado y aprobado en SEPTIEMBRE, 2021, como requisito previo para optar al título de máster en DIRECCIÓN EMPRESARIAL y reconociendo que la presentación del presente documento forma parte de los requerimientos establecidos del programa de maestrías de la Universidad Tecnológica Centroamericana (UNITEC), por este medio autorizo a las Bibliotecas de los Centros de Recursos para el Aprendizaje y la Investigación (CRAI) de UNITEC, para que con fines académicos puedan libremente registrar, copiar o utilizar la información contenida en él, con fines educativos, investigativos o sociales de la siguiente manera:

- 1) Los usuarios puedan consultar el contenido de este trabajo en las salas de estudio de la biblioteca y/o la página Web de la Universidad.
- 2) Permita la consulta y/o la reproducción a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato CD o digital desde Internet, Intranet, etc., y en general en cualquier otro formato conocido o por conocer.

De conformidad con lo establecido en los artículos 9.2, 18, 19, 35 y 62 de la Ley de Derechos de Autor y de los Derechos Conexos; los derechos morales pertenecen al autor y son personalísimos, irrenunciables, imprescriptibles e inalienables. Asimismo, el autor cede de forma ilimitada y exclusiva a UNITEC la titularidad de los derechos patrimoniales. Es entendido que cualquier copia o reproducción del presente documento con fines de lucro no está permitida sin previa autorización por escrito de parte de UNITEC.

En fe de lo cual se suscribe el presente documento en la ciudad de Tegucigalpa a los 27 días del mes de septiembre del año 2021.



---

**Ruth María Vásquez Portillo**  
**1203223**

**\* La autorización firmada se encuentra adjunta a mí expediente**



## **FACULTAD DE POSTGRADO**

### **Evolución de las tarjetas de crédito como medio de pago seguro**

**Ruth María Vásquez Portillo**

#### **Resumen**

El desarrollo del presente estudio de investigación hace referencia al origen y evolución de la tarjeta de crédito tanto a nivel mundial, Honduras para finalmente indicar el desarrollo de este instrumento en la ciudad de Tegucigalpa, con la finalidad de evaluar el conocimiento de los usuarios activos en relación a los protocolos de seguridad de su tarjeta de crédito para determinar acciones focalizadas en la formación e instrucción del usuario en relación al uso efectivo de las tarjetas, mitigando riesgos y fortaleciendo la utilización de las mismas como un medio de pago seguro. Los resultados derivan directamente de la evidencia recopilada a través del tipo de investigación con un alcance explicativo considerando que el mismo pretende establecer las causas del riesgo en las tarjetas de crédito como medio de pago seguro por medio de una metodología mixta realizando la recolección de datos por medio de la aplicación de entrevista/encuesta, evidenciando los usuarios desconocer los estándares de seguridad, afirmando solo el 18.5% conocer la evolución de los mismos siendo latente los posibles fraudes, por lo que es necesario redefinir la combinación de canales para la efectiva comunicación de protocolos y/o medidas de seguridad que incluyan información holística de sus tarjetas de crédito.

**Palabras claves: Banda magnética, blasters, estándares de seguridad, sistema EMV, volumen transaccional.**



## **GRADUATE SCHOOL**

### **Evolution of credit cards as a secure means of payment**

**Ruth María Vásquez Portillo**

#### **Abstract**

The development of this research study refers to the origin and evolution of the credit card both worldwide, Honduras to finally indicate the development of this instrument in the city of Tegucigalpa, in order to evaluate the knowledge of active users in relation to the security protocols of their credit card to determine actions focused on the training and instruction of the user in relation to the effective use of the cards, mitigating risks and strengthening the use of them as a secure means of payment. The results derive directly from the evidence collected through the type of research with an explanatory scope considering that it aims to establish the causes of risk in credit cards as a means of secure payment through a mixed methodology by collecting data through the application of interview / survey, evidencing users unaware of security standards, affirming only 18.5% know the evolution of the same being latent possible frauds, so it is necessary to redefine the combination of channels for the effective communication of protocols and / or security measures that include holistic information of their credit cards.

**Keywords: Blasters, EMV system, magnetic stripe, security standards, transactional volume.**

## **DEDICATORIA**

Con toda entereza está dedicado a uno de los pilares fundamentales de mi vida mi familia por su apoyo incondicional cada día para concretar dicho anhelo, a mis padres en reciprocidad por cada esfuerzo e inversión brindada y su respaldo integral en mi pregrado, e igual es dedicado a Nathaly Cerrato y Karla Peña personas que fueron relevantes en este ciclo de aprendizaje quienes me brindaron su apoyo en cada asignación que emprendíamos con expectativas de aprobar satisfactoriamente a través de un trabajo colaborativo y/o en equipo.

## **AGRADECIMIENTO**

Mi gratitud primeramente a mi Padre Celestial por manifestarme su respaldo brindándome la fuerza y sabiduría para concretar esta nueva etapa de crecimiento profesional y permitirme experimentar su gracia asombrosa palpablemente en todo este ciclo.

Agradezco a mis padres, familiares, compañeros y amigos que de una u otra forma fueron un aporte sustancial e incentivaron para la culminación de este logro importante en mi vida.

Manifiesto mi Agradecimiento a cada docente, que fue parte de mi enseñanza e instrucción a través de cada clase impartida con excelencia y la mayor diligencia para transferir su conocimiento siendo parte de mi formación en este ámbito.

# ÍNDICE DE CONTENIDO

DEDICATORIA .....	ix
AGRADECIMIENTO .....	x
ÍNDICE DE CONTENIDO .....	xi
CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN .....	1
1.1    Introducción .....	1
1.2    Antecedentes del Problema .....	1
1.3    Definición del Problema.....	4
1.4    Objetivos del Proyecto .....	5
1.5    Justificación.....	6
CAPÍTULO II. MARCO TEÓRICO .....	8
2.1    Análisis de la Situación Actual .....	8
2.1.1    Análisis del macroentorno .....	8
2.1.2    Análisis del microentorno.....	13
2.2    Conceptualización .....	14
2.3    Teorías de Sustento .....	16
2.3.1    Qué es el sistema EMV en las tarjetas.....	16
2.3.2    Cómo funciona el sistema EMV .....	16
2.3.3    Los cuatro fraudes más comunes con tarjetas de crédito .....	17
2.3.4    Banda magnética o chip en las tarjetas.....	17
2.3.5    Las ventajas del sistema EMV (o chip) en las tarjetas .....	18
2.3.6    Seguridad de las Tarjetas de Crédito .....	18
2.3.7    El futuro de las tarjetas EMV y tarjetas con chip .....	19
2.3.8    Categorías estándares a cumplir: .....	20
2.3.8.1    Construir y mantener una red segura .....	20
2.3.8.2    Proteger los datos del dueño de la tarjeta.....	20
2.3.8.3    Mantener un programa de gestión de vulnerabilidades .....	20

2.3.8.4 Implementar fuertes medidas de control de acceso .....	21
2.3.8.5 Monitorizar y probar las redes regularmente .....	21
2.3.8.6 Mantener una política de seguridad de la información .....	21
2.4 Análisis de las metodologías .....	21
2.4.1 Análisis crítico de las metodologías a emplear .....	23
2.5 Instrumentos Utilizados.....	24
2.6 Marco Legal .....	24
2.6.1 PCI Compliance, el estándar de seguridad para pagos online con tarjeta de crédito ...	24
2.6.2 PCI Compliance, el estándar de seguridad para pagos online con tarjeta de crédito ...	25
CAPÍTULO III. METODOLOGÍA .....	26
3.1 Congruencia Metodológica .....	26
3.1.1 Matriz de Congruencia .....	26
.....	26
3.1.2 Esquema de Variables .....	27
3.1.3 Operacionalización de Variables .....	28
3.2 Alcance, enfoque y métodos .....	29
3.3 Diseño de la Investigación .....	29
3.3.1 Población .....	29
3.3.2 Muestra .....	29
3.3.3 Unidad de Análisis .....	30
3.4 Técnicas, instrumentos y procedimientos aplicados .....	31
3.4.1 Técnicas .....	31
3.4.2 Procedimientos aplicados .....	31
3.5 Fuentes de Información.....	31
3.5.1 Fuentes Primarias .....	31
3.5.2 Fuentes Secundarias .....	31
CAPÍTULO IV. RESULTADOS Y ANÁLISIS .....	32
4.1 Análisis de resultados.....	32
4.1.1 Resultados obtenidos de las encuestas .....	32
4.2 Resultados obtenidos a partir de la entrevista .....	49
4.2.1 Experto encuestado director de tarjeta de crédito, Banco Davivienda Ing. Fabio	

Tabora.....	49
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES.....	54
5.1 Conclusiones .....	54
5.2 Recomendaciones.....	55
CAPITULO VI. APLICABILIDAD.....	57
6.1 Introducción .....	57
6.2 Nombre de la propuesta.....	57
6.3 Justificación de la propuesta .....	57
6.4 Alcance de la propuesta.....	58
6.4.1 Objetivos de la Implementación .....	58
6.5 Descripción y desarrollo de la propuesta .....	59
6.5.1 Plan de Acción empoderar usuario de tarjeta de crédito .....	63
6.5.2 Plan de Acción certificación y supervisor del riesgo por comercios con mayor volumen transaccional .....	64
6.6 Cronograma de actividades.....	65
6.6.1 Justificación del presupuesto .....	66
6.7 Tabla de concordancia.....	68
Manual de Medidas de seguridad- Introducción.....	73
REFERENCIAS BIBLIOGRÁFICAS.....	81
.....	82
ANEXOS .....	82

# **CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN**

## **1.1 Introducción**

En el país la evolución de las tarjetas de crédito como medio de pago ha cobrado vital importancia en los últimos años, generando un cambio en los patrones de consumo y pago, por esta razón se plantea el presente trabajo de investigación, cuya finalidad es determinar si en la población de la ciudad de Tegucigalpa, conocen las medidas de seguridad para utilizar estos medios de pago con la precaución para mitigar la vulnerabilidad de los delitos financieros generados por el uso del conocido dinero plástico.

El objetivo de esta investigación es evaluar el conocimiento de los usuarios financieros en relación a los estándares y/o protocolos de seguridad incorporados en sus tarjetas de crédito, por lo antes mencionado los resultados que se obtengan de la misma constituye un aporte significativo para las entidades financieras ya que proveerá información base del conocimiento de los usuarios financieros del producto otorgado, sus preferencias de consumo, canales de comunicación con mayor persuasión, marca que predomina, así como incentivar la adquisición de las tarjetas de crédito para aquellos usuarios financieros en potencia, interesados en realizar transacciones ágiles y seguras profundizando el tema de la seguridad en las transacciones a través de este medio de pago.

Con ello determinar acciones focalizadas en la formación del usuario financiero a través de la debida instrucción e información sobre el uso y las ventajas de estos medios de pago (Tarjetas de crédito) eliminando paradigmas de la complejidad del uso de los mismos en relación a los ya existentes.

## **1.2 Antecedentes del Problema**

Las tarjetas de crédito, surgieron a comienzos del siglo XX, cuando hoteles en Estados

Unidos emitían tarjetas a sus usuarios más frecuentes, convirtiéndose dichos negocios en las primeras empresas emisoras de tarjetas de crédito.

Sin embargo, el verdadero concepto de la tarjeta de crédito, fue concebido en la ciudad de Nueva York a mediados de los años 40, cuando Frank McNamara fundó un club para poder asistir a restaurantes de calidad sin tener que traer consigo dinero en efectivo, y a su vez una organización que garantizaría la cancelación de los consumos efectuados por los socios a los diferentes restaurantes y ésta a su vez se encargaría de cobrar a los diferentes socios.

Con la creación de dichas empresas y el nuevo enfoque otorgado a las tarjetas de crédito, comenzó una nueva era en la evolución del dinero, en la que el dinero papel se traslada dinero plástico el que ha venido a facilitar las transacciones comerciales y el cambio de bienes y servicios, aparte de brindar a sus usuarios seguridad en sus transacciones ya que se elimina la necesidad de portar grandes cantidades de dinero para realizar sus diferentes compras. A esta organización se le llamó Diners Club, que en español se traduciría como el "Club de los comensales.

Hoy en día se aprecia un cambio importante en los patrones de pago de la población, la creación de diversos instrumentos por parte de las entidades financieras y empresas en general para facilitar el pago de sus clientes, provoca que las tarjetas de crédito se constituyan actualmente en el mecanismo de mayor uso a nivel mundial.

Con la finalidad de conocer el comportamiento que se presenta con el uso de tarjetas de crédito como medio de pago, así como para describir los principales factores que inciden en el proceso de generación de deuda derivado del uso de este mecanismo de pago (Loaiza, 2014) emplea la herramienta de investigación mediante la aplicación de una encuesta que contiene 21 preguntas 4 de la mismas relacionadas con datos generales y 17 se relacionan con información financiera de cada encuestado.

Obteniendo como resultado que Cerca del 60% de los encuestados mantienen niveles de gastos óptimos, los cuales, de acuerdo a la información proporcionada por ellos, se ubican en un 40% de sus ingresos, incluidos aquí deudas en general. Mientras que, un 13% de la población se encuentra en el umbral de riesgo elevado, ya que del total de ingresos que perciben el 100% lo destinan al pago de sus deudas, cayendo por tanto en niveles de sobreendeudamiento general, más no originado por uso de tarjetas de crédito.

La actividad comercial evolucionó a pesar de que en nuestros días el empleo del cheque junto con la letra de cambio y el pagaré sigue siendo una práctica regular en el comercio, en lo que respecta al mundo de las economías domésticas una nueva forma de pago ha emergido durante el siglo XX como modo de reducir el manejo de efectivo y con el ánimo de facilitar el comercio en todo el mundo, las tarjetas de pago conocidas como "dinero plástico".

De esta forma las tarjetas de crédito se han convertido en un medio de referencia de casi obligada aceptación en la compra de bienes y servicios y ha sido el último paso en la evolución histórica de los sistemas de pagos teniendo como pilar básico la utilización de la tarjeta de crédito como financiador de operaciones de consumo tal como lo expresa el estudio realizado por (MATA, 2009) .

Utilizando el diseño del proceso de investigación empírica clasificación de las fuentes, cuestionario, dimensión temporal obteniendo como resultado que las entidades consideran al uso dado de las tarjetas como incorrecto ya que en su opinión de deberían utilizar más en compras se comprobó que el uso del efectivo ha sido un factor limitante para el uso de las tarjetas en compras.

Es relevante poder acercar la investigación científica con la investigación aplicada por (OLAVARRIETA, 2012) de modo de poder evaluar acciones concretas para buscar un desarrollo y crecimiento más efectivo siendo de gran utilidad para los tomadores de decisiones poder disponer

de metodologías que permitan proyectar comportamientos frente a la aplicación de normas o estándares y sus efectos.

Lo anterior permitirá poder hacer acciones focalizadas para mitigar riesgos o fortalecer servicios como una mayor eficiencia en el uso de estos medios de pago aplicando estándares y sus efectos en la industria de Chile utilizando el modelo investigativo de regresión simple que sirve para encontrar ponderaciones aún mejores para que las estimaciones sean lo más precisas posibles y el modelo regresión múltiple que incorpora las diferencias porcentuales entre los valores esperados dados por el modelo de regresión y los datos reales.

La aplicación de la metodología aplicada en dicho estudio dio como resultado una mayor estandarización interoperabilidad y confiabilidad acercando así a oferentes y demandantes lo que permitirá una atomización mayor del comercio internacional y en el futuro una mayor diversificación.

### **1.3 Definición del Problema**

En el país la evolución de este medio de pago ha cobrado vital importancia en los últimos años, generando un cambio en los patrones de consumo y pago, por esta razón se plantea el presente trabajo de investigación, cuya finalidad es determinar si en la población de la ciudad de Tegucigalpa se conocen las medidas de seguridad para utilizar estos medios de pago con la precaución para mitigar la vulnerabilidad de los delitos financieros generados por el uso del conocido dinero plástico.

Con la formación del usuario financiero a través de la debida instrucción e información sobre el uso y las ventajas de estos medios de pago (Tarjetas de crédito) eliminando paradigmas de la complejidad del uso de los mismos en relación a los ya existentes.

## **Pregunta Problema de Investigación**

¿Cuáles estrategias son efectivas para empoderar a los usuarios de tarjeta de crédito en relación a la seguridad de las transacciones realizadas a través de este medio de pago?

## **Pregunta Problema de Investigación**

1. ¿Existen estándares de seguridad en la industria de medios de pago y/o tarjetas créditos?
2. ¿Cuáles son las fechas de utilización con mayor riesgo en la industria de pago y/o tarjetas créditos?
3. ¿Las medidas de seguridad aplicadas contienen riesgo operativo en las transacciones?
4. ¿Los usuarios financieros conocen los estándares y/o medidas de seguridad de sus tarjetas de crédito?

## **1.4 Objetivos del Proyecto**

### **Objetivo General**

Determinar acciones focalizadas en la formación e instrucción del usuario en relación al uso efectivo de las tarjetas, mitigando riesgos y fortaleciendo la utilización de las mismas como un medio de pago seguro.

### **Objetivo Especifico**

1. Identificar estándares de seguridad aplicados en la industria de los medios de pago para las tarjetas de crédito.
2. Determinar efectos sobre volumen transaccional identificando fechas específicas con

mayor riesgo.

3. Describir los actuales puntos fuertes y débiles en los estándares o medidas de seguridad aplicadas.
4. Evaluar el conocimiento de los usuarios activos en relación a los protocolos de seguridad para desarrollar un manual guía y/o instructivo que contenga estrategias de comunicación para empoderarlos, permitiendo detectar barreras o vulnerabilidad, que pueda condicionar la efectividad de una eficaz y segura transacción, que limite la utilización de las misma.

### **1.5 Justificación**

El desarrollo del presente estudio de investigación hace referencia al origen y evolución de la tarjeta de crédito tanto a nivel mundial, en América Latina, Honduras para finalmente indicar el desarrollo de este instrumento en la ciudad de Tegucigalpa.

Estos datos proveen una base inicial para posteriormente incluir datos relacionados con el tema de investigación planteado, para ello se incluirá información sobre estudios similares realizados en otros países de América Latina, abordados desde la perspectiva financiera y de seguridad de este medio de pago. Estos datos proveen una primera aproximación para poder dar respuesta a la pregunta planteada.

Así mismo, se espera disponer de información estadística histórica hasta la actualidad de la evolución de las tarjetas de crédito con la inclusión progresiva de estándares o medidas de seguridad a nivel mundial, Honduras y de manera especial de la ciudad de Tegucigalpa. Disponiendo de esta información se podrá establecer cómo se encuentra el uso de tarjetas de

crédito y la confianza del usuario como medio de pago en la ciudad de Tegucigalpa.

El levantamiento de la información de fuentes primarias constituye un elemento fundamental para poder establecer las relaciones de causa-efecto del problema planteado, por lo tanto, se espera que de la muestra seleccionada las personas entrevistadas provean información veraz referente a las formas de pagos, usos de tarjeta de crédito, entre otros elementos que, aunque se constituye datos sensibles y personales, son necesarios para poder alcanzar los objetivos planteados.

Por esta razón los resultados que se obtengan de esta investigación constituye un aporte significativo para las entidades financieras ya que proveerá información base del conocimiento de los usuarios financieros del producto otorgado, así como incentivar la adquisición de las tarjetas de crédito para aquellos usuarios financieros en potencia interesados en realizar transacciones ágiles y seguras profundizando el tema de la seguridad en las transacciones a través de este medio de pago en la ciudad de Tegucigalpa como a nivel nacional.

## **CAPÍTULO II. MARCO TEÓRICO**

### **2.1 Análisis de la Situación Actual**

#### **2.1.1 Análisis del macroentorno**

El presente Marco Teórico hace referencia al sistema financiero de Honduras en cuanto a su origen, evolución en los últimos años.

Así mismo incluye aspectos sobre la evolución de las tarjetas de crédito a nivel mundial en América Latina para finalmente indicar el desarrollo de este instrumento.

Estos datos proveen una base inicial para posteriormente incluir datos relacionados con el tema planteado, para ello se incluirá información sobre estudios similares realizados en otros países de América Latina, abordados desde la perspectiva de seguridad económica y financiera, estos datos proveen una primera aproximación para dar respuesta a la pregunta planteada.

Las tarjetas de crédito, son planes de ventas a crédito de mucho uso y trascendencia en la actualidad, ya que provee al consumidor de varios privilegios para obtener productos y servicios a crédito, un medio de pago sin uso de efectivo, con un financiamiento automático a treinta días, sin costo.

La primera tarjeta de crédito utilizada fue la Diners Club, Inc. en el año mil novecientos cincuenta, la cual estableció un sistema por medio del cual se otorgaba al dueño de la tarjeta, una cantidad máxima de consumo mensual o anual y se le daba un comprobante firmado.

En el año mil novecientos sesenta y seis en donde el Bank of América, emitió una nueva tarjeta llamada BankamericaCard, la cual estableció una variante que respaldaba al comerciante, ya que el tarjetahabiente pagaba al banco.

En el año mil novecientos setenta y siete, el sistema de BankamericaCard contaba con oficinas bancarias y de comercios afiliados en ciento diecisiete países, y se lanza al cambio del

nombre más grande e importante de la historia de las tarjetas de crédito –VISA

La tarjeta de crédito, surgió en Guatemala en los años sesenta a través de Cuentas, S. A., una sociedad constituida con un capital guatemalteco. Inicialmente, esta sociedad fue creada con el objeto del manejo de una tarjeta de crédito a nivel local. Posteriormente aparece en Guatemala la tarjeta de crédito de Diner's Club, la primera tarjeta de crédito internacional representada en Guatemala

A partir del año mil novecientos setenta y ocho, apareció Credomatic de Guatemala, S. A., representando las marcas Visa, Master Card y una tarjeta de uso local.

Es así como a partir del año mil novecientos noventa y nueve, el mercado de las tarjetas de crédito inicia su crecimiento y evolución en el país, que de acuerdo a la empresa emisora o coemisor ofrecen una diversidad y tipos de tarjetas conforme a las necesidades y expectativas de las personas. (matefinanciera1, 2015)

La importancia de un sistema financiero y la función de los bancos para la prosperidad de los países ha sido aceptada desde hace tiempo en el análisis económico.

Resultan fundamentales para la evolución general de una economía, siendo su misión realizar una eficaz asignación de los recursos económicos, lograr tanto la estabilidad monetaria como financiera y proporcionar una seguridad máxima en los sistemas de pago. Los bancos desempeñan un papel central dentro de las instituciones que conforman el sistema financiero, es por ello su alta participación e influencia en la actividad económica de los países.

Los bancos cumplen una función muy específica en la economía de libre mercado, como es actuar de intermediarios financieros entre ofertantes y demandantes de fondos. Por un lado, tienen la capacidad de estimular y recibir el ahorro de una sociedad, y por otro, distribuirlo entre

los agentes económicos que lo necesitan para llevar a cabo sus actividades de consumo e inversión.

Desde estas consideraciones se puede decir que un sistema financiero es un todo estructurado, compuesto por un conjunto de instituciones, activos, mercados y técnicas específicas cuyo objetivo principal es el de canalizar el ahorro desde las unidades económicas con superávit hacia aquellas unidades que tienen déficit. Dentro del sistema financiero se puede definir sencillamente a los bancos como una institución de intermediación financiera cuyas principales operaciones consisten en recibir depósitos de los ahorradores y, por otro, otorgar préstamos o tarjetas de créditos a los demandantes, es decir, a los agentes económicos. (Bejar, 2012)

El estándar de seguridad de datos PCI DSS se aplica para cualquiera que almacene, procese o transmita información de un usuario de algún tipo de tarjeta, así como también a todos los sistemas técnicos y operacionales que se encuentran conectados o incluidos a la red de pagos.

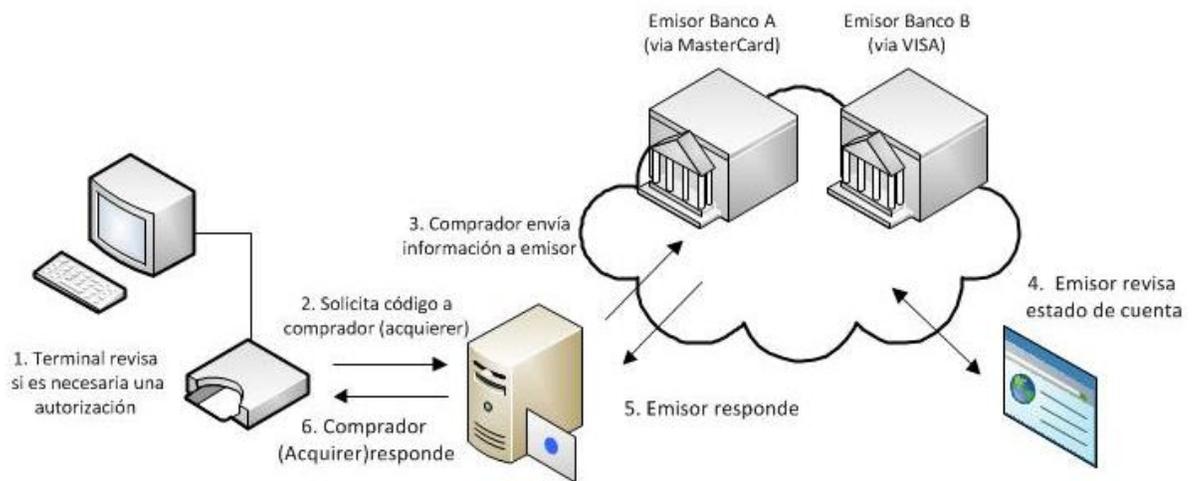


Figura 1: Flujo de información en una transacción con una tarjeta de pago

Un antecedente a destacar en agosto del 2009, por el Departamento de Justicia de Estados Unidos donde anunció la detención de un hombre residente de Florida que robó 130 millones de

números de tarjetas de crédito y débito, considerado uno de los mayores de la historia. Este hombre accedió ilegalmente a los sistemas informáticos de la compañía de manejo de pagos por internet Heartland Payment Systems, que ofrecía sus servicios a las cadenas de establecimientos 7-Eleven y a la cadena de supermercados Hannaford Brothers.

Incidentes como estos generaron la presión y demandas por parte de los usuarios para la consolidación de estándares de seguridad como PCI DSS para garantizar la privacidad de la información de los clientes de este tipo de tarjetas de pago. En la actualidad, las compañías que no implementen este tipo de estrategias, son perseguidas y penalizadas por entes gubernamentales. (Vieda, 2010)

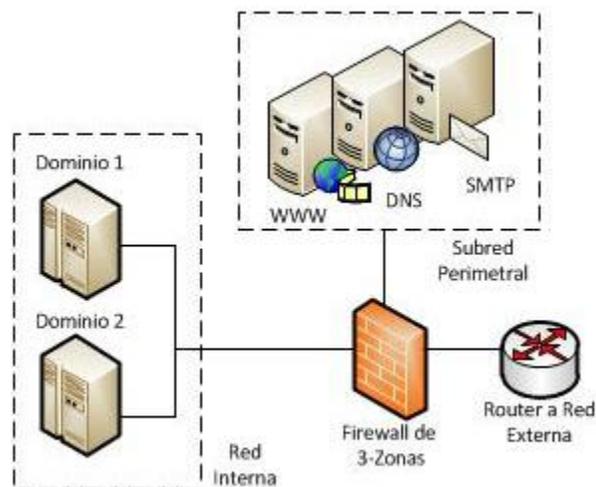


Figura 2 Implementación de Firewall donde la información sensible se encuentra protegida de acceso no autorizado.

Los riesgos de seguridad digital que merecen la mayor atención por parte de las entidades bancarias son: a) el robo de base de datos crítica, b) el compromiso de credenciales de usuarios

privilegiados, y, c) la pérdida de datos. (asociacion de los estados mericanos , 2018)

GoNetFPI y 1st Secure IT Plantean alianza para luchar contra el fraude en medios de pago en el mercado ibérico en el que les permite ofrecer la máxima seguridad a sus clientes que operen con medios de pago tanto en el mercado ibérico como en el europeo y latinoamericano. Para ello, la alianza cuenta con un equipo dedicado en exclusiva a esta actividad y que está apoyado en todo momento por un grupo con más de 20 expertos auditores internacionales certificados como QSA por el PCI Council.

El número de españoles con al menos una tarjeta en su posesión alcanzó en 2017 al 82% de la población, lo que se tradujo en un aumento de ocho puntos porcentuales en relación al dato registrado un año antes y supone el dato más alto de toda la serie histórica desde hace 30 años, según una encuesta realizada por MasterCard. Actualmente en el mercado ibérico hay más tarjetas que habitantes de ahí que sean uno de los focos de los ciberdelincuentes y la necesidad de proteger las operaciones que se realizan con las mismas. La ciberdelincuencia ha encontrado uno de sus nichos y de ahí la importancia de ofrecer los servicios más completos y seguros para proteger los medios de pago de posibles ataques. (IT DIGITAL SECURITY, 2018, pág. 3)

Según lo indica ADICAE, la experiencia del usuario, Tiene que tener claro que, entre los diversos medios de pago electrónico, son los pagos inmediatos los que se convertirán en el principal campo de desarrollo a corto plazo. La inmediatez y la seguridad que brindan, esto les convierte en la principal apuesta europea, que con seguridad seguirá creciendo en protagonismo y avanzando a nivel global. Lo inmediato e instantáneo va ligado al comercio electrónico y a la banca móvil. Ahora la propia regulación europea aspira a que las entidades financieras adapten los tiempos de atención y operatividad de sus canales, orientándonos hacia un modelo que le dé continuidad a los servicios de pago 24/7, de modalidad online, interactiva e interconectada, de

diferido a inmediato, aumentando las demandas de confiabilidad para los PSP y sistemas de pagos.  
(ADICAE, 2019)

### **2.1.2 Análisis del microentorno**

La historia de la banca privada en Honduras comenzó en el año de 1889, cuando se otorgó la autorización para fundar dos bancos comerciales que se denominaron Banco Centro-americano y Banco Nacional Hondureño, ambos con la facultad de emitir billetes.

Estos dos bancos se fusionaron el 10 de octubre de ese año para formar lo que hoy se conoce todavía como el Banco de Honduras", con un capital inicial de 400,000 lempiras. Posteriormente, en la costa norte del país y bajo la influencia del desarrollo de la industria bananera en Honduras, en especial de Vaccaro Brothers and Company, en el año de 1912 se estableció un banco en la ciudad de la Ceiba, departamento de Atlántida, bajo la denominación Banco Atlántida. Este banco estaba facultado para abrir sucursales en la costa norte, específicamente en los departamentos de Atlántida, Yoro y Colón, y podía emitir dinero con la firma del ministro de Hacienda.

También surge el Banco de Comercio que se autoriza el 31 de enero de 1913. El Banco de Comercio es autorizado para emitir billetes hasta su liquidación en 1917 cuando es comprado por el banco Atlántida. Desde 1917 hasta 1950 solo los billetes del Banco Honduras y del Banco Atlántida circulan en el país.

Las reglas bajo las cuales se les permite operar a los primeros dos bancos privados en 1888 y que pasan al Banco de Honduras en 1889 se consideran prudentes. Estas reglas se modifican en cuanto al encaje. En 1915 el Banco de Comercio aumenta su capital y solicita la emisión de billetes, el gobierno lo faculta.

Hasta estos momentos, el sistema monetario de Honduras se inscribe en el patrón plata y

consta de dos aspectos: la emisión de moneda metálica con el peso y la ley de la legislación de 1879 y la emisión de papel moneda por parte de los bancos privados con las restricciones contenidas en cada concesión particular.

La moneda que se utiliza en Honduras, es el lempira que sustituyó a la que era anteriormente y se denominaba peso hondureño. Es el denominado Banco Central de Honduras el encargado de regir la política monetaria del país, siendo la autoridad monetaria y crediticia de Honduras se encarga también de la fiscalización de los bancos en Honduras nacionales y extranjeros.

Las operaciones bancarias en Honduras son accesibles a toda la población, la banca de Honduras permite la realización de todo tipo de operaciones bancarias a nivel nacional e internacional para las entidades jurídicas como individuales y también tiene una gran cobertura de banca online. (Castro, 2016).

## **2.2 Conceptualización**

**Contactless:** es el término que se aplica a la tecnología que permite realizar operaciones ‘sin contacto’ mediante un sistema de comunicación denominado NFC (‘near field communications’). Se utiliza principalmente con tarjetas de crédito, pero cada vez hay más dispositivos plásticos que admiten esta tecnología, como teléfonos móviles, relojes inteligentes o llaveros.

**Código CVV** (Código de validación) es el grupo de tres o cuatro dígitos, tradicionalmente en cursiva, sirve como medida adicional de seguridad. Conocer este código garantiza que el titular tiene físicamente la tarjeta, se utiliza en transacciones electrónicas o compras en internet

**Banda Magnética:** Contiene información de la tarjeta, la misma es recibida por el terminal POS al momento de ser deslizada para compras en comercio.

**Chip de seguridad sistema EMV:** protección creando un código único y exclusivo para cada transacción.

**Número de identificación:** Es una serie de dígitos único.

**La tokenización:** es el proceso que permite proteger datos sensibles, sustituyéndolos por equivalentes no-sensibles, conocidos como tokens. Un token en sí no tiene ningún valor o significado, es una referencia o identificador que, gracias al sistema de tokenización, permite volver al dato sensible. La tokenización se utiliza para evitar el robo de datos en las transacciones con tarjetas bancarias.

**Fecha de vencimiento:** Posterior de esta fecha se inhabilita la utilización.

**Variables:** son esencias aspectos o características de algo, que pueden ser observados y que adoptan un determinado valor o categoría, a través de cual se expresan o manifiestan. Las variables son de vital importancia constituyéndose en la columna vertebral de todo el proceso de investigación, pues ellas operan en todas las fases finales de la investigación.

**Indicadores:** es una sub-variable que se desprende con el propósito de ser medición cualitativa o cuantitativa, los indicadores dan lugar a procedimientos de observación y precisión de datos necesarios para cada variable de modo que al interior de las variables encontramos los indicadores y al interior de estos los datos. (non-commercial(BY-NC), 2013)

## **2.3 Teorías de Sustento**

### **2.3.1 Qué es el sistema EMV en las tarjetas**

Es decir que las ventajas que desarrolla esta tarjeta es la búsqueda de mayor seguridad en las transacciones entre tarjetas y terminales, ya que la tarjeta EMV valida las operaciones gracias a la información almacenada en su chip.

Cabe aclarar que EMV es un nuevo estándar de medios de pago (tanto crédito como débito) definido por MasterCard y Visa que se caracteriza principalmente por estar basado en la tecnología chip. A diferencia de la banda magnética, este chip es un elemento activo de seguridad, ya que es la propia tarjeta la encargada de evitar su manipulación garantizando su autenticidad.

Por lo tanto, se reducen las acciones de fraude, que con tarjetas de crédito de barra magnética (aunque es un poco más lento por la cantidad de cálculos criptográficos) se producen a diario y además se puede tener un mayor control en la aprobación de los pagos sin conexión.

### **2.3.2 Cómo funciona el sistema EMV**

De esta manera, cuando se introduce la tarjeta con chip en la terminal, se autentica y permite a los terminales compatibles con el estándar EMV comprobar la validez de la tarjeta. Además, este tipo de tecnología EMV brinda la posibilidad de comprobar que el usuario sea realmente el titular de la misma la tarjeta que está utilizando. Y por si no fuera suficiente, evalúa el riesgo a partir de parámetros que el emisor ha introducido en el chip, así como los de la compañía emisora de tarjetas que el distribuidor o el proveedor del terminal han introducido en nombre de esta entidad. De esta forma, esta tecnología aporta mayor seguridad a las transacciones porque tramita la compra por medio del chip, el cual no puede ser clonado, tal como sucede con la banda magnética, y exige al titular teclear su clave. Evidentemente aumentar los niveles de seguridad de las tarjetas resulta un

elemento básico para un mejor control de las finanzas personales.

### **2.3.3 Los cuatro fraudes más comunes con tarjetas de crédito**

Esta nueva tendencia mundial lleva a la utilización en masa del sistema EMV, aunque los plásticos con bandas magnéticas seguirán utilizándose. Además, cabe destacar que estas tarjetas incorporan el chip, pero no dejan de tener banda magnética por lo que son aceptadas en todos los comercios y cajeros a nivel mundial.

Tal es así que el Euro sistema tomó la decisión que todas las tarjetas emitidas desde 2012 tendrán que contar con este sistema de seguridad EMV o chip, con lo cual todos los plásticos pasarán a tarjetas sólo chip, dejando atrás por siempre la banda magnética. Asimismo, cabe destacar que este chip es obligatorio en toda Europa a partir de 2011.

### **2.3.4 Banda magnética o chip en las tarjetas**

Como el tiempo se está encargando de demostrar no estamos ante un sistema sustitutivo, de hecho, el grueso de estas tarjetas inteligentes viene combinándose con el uso de la banda magnética.

En primer lugar, se tiene que tener en cuenta que la banda magnética es una tecnología incorporada a las tarjetas de crédito desde prácticamente cuatro décadas atrás. Partiendo de un funcionamiento rudimentario en el que estas bandas magnéticas almacenaban datos en una tira de plástico y sentada en la tarjeta con un revestimiento de óxido de hierro (que generaba los datos en la lectura) aunque ha evolucionado en cuanto a materiales y aplicación tecnológica, no ha evolucionado excesivamente como concepto.

Este hecho hace que, lógicamente, casi cuatro décadas de tecnología similar haya generado por parte de los usos fraudulentos, una auténtica colección de opciones para clonar tarjetas, robar datos de la tarjeta o simplemente hacer uso fraudulento.

En la búsqueda alternativa de soluciones en combinación a la banda magnética aparece el sistema EMV.

### **2.3.5 Las ventajas del sistema EMV (o chip) en las tarjetas**

Evidentemente sobre la principal ventaja de este sistema descansa en el hecho de aumentar la seguridad a diferencia de la banda magnética que almacena datos en la propia tarjeta, el uso de un chip incorporado fue ganando peso en los últimos años del pasado siglo cuando se hizo patente que esta tecnología garantizaba mayores niveles de seguridad.

El almacenamiento de la información en los chips, y la necesidad de respuesta por parte de los dispositivos que se utilicen para generar la autorización de la tarjeta, hacía que este uso de un pequeño microprocesador incorporado a las tarjetas resultara más eficaz, y, de hecho, poco a poco, en muchos países ha ido desplazando a los tradicionales sistemas lectores de tarjetas, que, si bien aún siguen existiendo son una suerte de dispositivo en desuso cara al futuro.

Replicar este tipo de tarjetas resulta mucho más complejo que la clonación de una tarjeta de uso exclusivo con banda magnética. Sólo por esto los niveles de seguridad ya resultan mucho más elevados, y, a esto debemos sumar el hecho de los diferentes modelos de funcionamiento recordando que las tarjetas no sólo tienen su propio chip inteligente sino también poseen niveles añadidos de seguridad empezando por los propios números de identificación personal que no se eliminan.

### **2.3.6 Seguridad de las Tarjetas de Crédito**

Los inconvenientes de las tarjetas con sistema EMV (o chip) el principal problema estriba en un hecho universal: no hay una protección garantizada de manera total para nuestras tarjetas en ningún caso.

Es en la combinación de elementos de seguridad de las tarjetas, los dispositivos, y en el

uso adecuado de las tarjetas por parte del usuario donde vamos a encontrar elementos para minimizar los riesgos, pero éstos seguirán existiendo.

Evidentemente desplazar el riesgo de duplicado mecánico inherente a las tarjetas de banda magnética ya es un logro, pero, esta tecnología a un tiene vulnerabilidades como por ejemplo los ataques de malware destinados a la obtención de datos que no son mitigados por el uso de estas tarjetas ya que debemos recordar que no todas las transacciones que podemos realizar requiere la presencia física de la tarjeta, es decir, simplemente utilizando software malicioso para la captación de datos (algo a lo que nuestras tarjetas son vulnerables) o utilizando dicho software para la obtención de datos personales como el número privado de acceso a la tarjeta, el delincuente puede llegar a utilizar de manera fraudulenta nuestras tarjetas.

Resulta muy importante tener en cuenta esto ya que, si efectivamente estas tarjetas con chip son muy eficaces en el uso presencial, hoy en día una gran mayoría de fraudes con tarjetas se cometen precisamente en operaciones o en acciones en las que la tarjeta no está presente y se utiliza tan sólo los datos.

### **2.3.7 El futuro de las tarjetas EMV y tarjetas con chip**

En los últimos 20 años las vulnerabilidades de las tarjetas es el hecho de la necesidad de evolucionar de manera constante en los sistemas de protección.

Mantener una tecnología mucho tiempo sin evolucionar significa exponer cada vez de manera exponencial los riesgos de encontrar vulnerabilidades. En el futuro los modelos de pago, que parece que evolucionan cada vez más al uso no físico de las tarjetas, irán acompañados de sistemas de seguridad y barrera entre las tarjetas (los chips) y los dispositivos de cobro, buscando cada vez más la eficacia de ambas cuestiones.

Por otro lado hemos ido contemplando a lo largo del tiempo también la evolución en el uso

de las tarjetas es el punto de vista práctico, con experiencias de todo tipo incluyendo por ejemplo las que buscan aumentar la presencia del usuario las transacciones a través, por ejemplo, de iniciar sesión en las cuentas bancarias asociadas a la tarjeta, como un elemento de protección añadidos, algo en práctica ya en algunos países del mundo de manera rápida y sencilla, y sobre todo añadiendo aún más niveles de garantía y seguridad. (NVINDI, 2019)

### **2.3.8 Categorías estándares a cumplir:**

#### **2.3.8.1 Construir y mantener una red segura**

Las normativas de esta categoría se enfocan en la red en la cual se exponen los datos de la tarjeta. En los eCommerce el primer foco es el servidor web. Las compañías de hosting deben encargarse directamente de asegurar los servidores web que alojan los sitios de sus clientes.

Para lograrlo deberán instalar y mantener una configuración de firewall para proteger los datos y no usar los passwords o parámetros de seguridad que vienen por defecto en los sistemas, reforzando así la seguridad de los mismos.

#### **2.3.8.2 Proteger los datos del dueño de la tarjeta**

Para cumplir con este punto es necesario que, al recolectar los datos del dueño de la tarjeta de crédito, estos se almacenen cifrados para que en caso de robo no puedan ser accesibles de manera directa. Se debe utilizar un certificado SSL de 128 bits para proteger la información que se ha recolectado.

#### **2.3.8.3 Mantener un programa de gestión de vulnerabilidades**

Tener actualizados al día los antivirus, ejecutar los escaneos y cumplir con un plan de gestión de actualizaciones de hardware, software y sistemas operativos puede disminuir el riesgo de tener vulnerabilidades en el sistema.

#### **2.3.8.4 Implementar fuertes medidas de control de acceso**

Una de las normas más importantes del PCI Compliance es controlar que solo las personas que necesiten la información tengan el acceso a ella, no importando si es de manera física o virtual. Se debe restringir y limpiar el acceso a la información de las tarjetas mediante los permisos mínimos necesarios, asignar un ID único a cada persona con acceso a un PC y restringir el acceso físico a las tarjetas.

#### **2.3.8.5 Monitorizar y probar las redes regularmente**

Para solucionar y detectar potenciales fallos de seguridad es necesario monitorizar y probar las redes que mantienen la información confidencial de los dueños de las tarjetas de crédito, igualmente se debe revisar recurrentemente los accesos a los recursos de red y probar los sistemas de seguridad.

#### **2.3.8.6 Mantener una política de seguridad de la información**

Se deberá estar seguros de que los empleados conozcan los puntos de la política de seguridad que se aplique al igual que las responsabilidades que se tienen con los datos de los dueños de las tarjetas. Para cada uno de estos requerimientos existen varios servicios e infraestructuras de apoyo que están orientados a la seguridad del manejo de los datos sensibles a la hora de cobrar con tarjetas de crédito y por ende a cumplir con las normas del PCI Compliance. (Galeano, 2016)

### **2.4 Análisis de las metodologías**

A través de este estudio se podrá explorar la formación y la instrucción a la evolución de las medidas de seguridad de la tarjeta de crédito como medio de pago y la relación con el comercio electrónico y sus efectos en el mercado.

El objetivo de la investigación es encontrar relaciones entre la implementación de medidas

de seguridad y la mayor confianza en el uso de las tarjetas de crédito de los tarjetahabientes en el mercado.

La aparición del dinero constituye uno de los grandes avances de la civilización humana en toda su historia. En nuestra sociedad moderna existen muchos instrumentos que cumplen esas funciones, tanto que en ocasiones resulta difícil distinguir si un cierto instrumento financiero es dinero o no. Además, la tecnología electrónica está impulsando la aparición continua de nuevos medios de pago lo que dificulta aún más la tarea de medir la cantidad de dinero que circula por un país.

La metodología implementada en el estudio realizado por (Cosios, 2010) se realizó a través de una investigación participativa con la población de la ciudad de Loja, tomando en cuenta para el análisis únicamente el sector urbano (El Valle, Sucre, El Sagrario, San Sebastián), la que permitió obtener información para determinar el medio de pago más utilizado por los demandantes en la ciudad de Loja.

Se realizó la recopilación de información secundaria, observación directa y la aplicación de encuestas dirigidas a los diferentes grupos ocupacionales, obteniendo como muestra 382, las cuales fueron calculadas de una población de 72,203 habitantes que corresponden a la población económicamente activa.

El proyecto planteado por (Loaiza, 2014) tiene la finalidad de conocer el comportamiento que se presenta con el uso de tarjetas de crédito como medio de pago, así como para describir los principales factores que inciden en el proceso de generación de deuda derivado del uso de este mecanismo de pago.

Dicho estudio es de tipo exploratorio, se reveló que existen únicamente ideas vagamente

relacionados con el problema planteado, por tal razón la necesidad de llevar a cabo este trabajo para tener una primera aproximación del comportamiento de los tarjetahabientes con el uso de sus tarjetas de crédito.

Se procedió a levantar información de fuentes directas datos que permitieron evaluar y establecer el comportamiento de uso de tarjetas de crédito como medio de pago en la ciudad de Loja, para tal propósito se elaboró una encuesta constituida por un total de 21 preguntas, de las cuales cuatro corresponden a preguntas relacionadas con variables demográficas tales como: género, edad, estado civil, actividad que realiza.

#### **2.4.1 Análisis crítico de las metodologías a emplear**

Considerando la evaluación de las teorías certificadas en estudios similares en las que se identifican diferentes metodologías empleadas una participativa con recopilación de información secundaria, observación directa y la aplicación de encuestas dirigidas a los diferentes grupos ocupacionales, la que permitió obtener información para determinar el medio de pago más utilizado por los demandantes.

Y una exploratoria ya que se reveló que existen únicamente ideas vagamente relacionados con el problema planteado, por tal razón la necesidad de llevar a cabo este trabajo para tener una primera aproximación del comportamiento de los tarjetahabientes con el uso de sus tarjetas de crédito procediendo a levantar información de fuentes directas datos que permitieron evaluar y establecer el comportamiento de uso de tarjetas de crédito como medio de pago aplicando una encuesta constituida por un total de 21 preguntas.

Considerando el análisis que antecede se determina emplear en la presente investigación un alcance explicativo ya que el mismo pretende establecer las causas del riesgo en las tarjetas de crédito como medio de pago seguro, con un enfoque en una metodología mixta realizando la

recolección de datos a través de entrevista/encuesta.

## **2.5 Instrumentos Utilizados**

En el sondeo y estudio realizado, los instrumentos utilizados revelados en la investigación de (Cosios, 2010) es un método cuantitativo se realizó mediante la aplicación de encuestas dirigidas a los diferentes grupos ocupacionales, obteniendo como muestra 382, las cuales fueron calculadas de una población de 72,203 habitantes que corresponden a la población económicamente activa.

En la investigación realizada por (Loaiza, 2014) se procedió a levantar información de fuentes directas se elaboró una encuesta constituida por un total de 21 preguntas, de la cuales cuatro corresponden a preguntas relacionadas con variables demográficas tales como: genero, edad, estado civil, actividad que realiza, para el diseño de la encuesta se tomaron encuesta razones de temporalidad.

## **2.6 Marco Legal**

### **2.6.1 PCI Compliance, el estándar de seguridad para pagos online con tarjeta de crédito**

PCI Compliance son las siglas que provienen de Payment Card Industry Compliance, que podría traducirse como Cumplimiento de la industria de tarjetas de pago.

Es decir, se trata de una serie de normas que han sido desarrolladas para proteger los datos proporcionados al comprar con tarjetas de crédito durante y después de cualquier transacción financiera. Este estándar de requerimientos de seguridad debe ser cumplido por quienes procesen pagos con tarjetas. No importa si tu comercio es nuevo o maneja poca cantidad de transacciones o utilizas proveedores externos para externalizar la información de las tarjetas de crédito de tus clientes, aun así, deberás cumplir con ciertos requisitos de verificación de las normas del PCI

Compliance.

### **2.6.2 PCI Compliance, el estándar de seguridad para pagos online con tarjeta de crédito**

La validación del PCI Compliance se lleva a cabo por auditores cualificados (Qualified Security Assessor o QSAs). Eso sí, en el caso de tiendas online pequeñas, con menos de 80,000 transacciones por año, se les permite realizar una autoevaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC).

Si no cumples con los requerimientos del PCI Compliance, podrías ser inhabilitado para procesar pagos con tarjetas de crédito.

Lo que pretenden con el programa de seguridad de datos denominado PCI Compliance es evitar el fraude con el pago de tarjetas. El grupo formado por American Express, Discover Financial Services, JCB International, MasterCard y Visa entre otras organizaciones suman esfuerzos para mejorar los estándares y vigilar el cumplimiento de las normas.

## CAPÍTULO III. METODOLOGÍA

### 3.1 Congruencia Metodológica

#### 3.1.1 Matriz de Congruencia

TÍTULO	PROBLEMA	PREGUNTAS DE INVESTIGACIÓN	OBJETIVOS ESPECÍFICOS	VARIABLES	
				INDEPENDIENTE	DEPENDIENTE
Evolución de las tarjetas de crédito como medio de pago seguro	¿Evaluar diferentes estrategias para empoderar a los usuarios de tarjeta de crédito en relación a la seguridad de las transacciones realizadas a través de este medio de pago?	¿Existen estándares de seguridad en la industria de medios de pago y/o tarjetas créditos?	Identificar estándares de seguridad aplicados en la industria de los medios de pago para las tarjetas de crédito	Estandares de seguridad	Tarjeta de Crédito como medio de pago seguro
		¿Cuáles son las fechas de utilización con mayor riesgo en la industria de pago y/o tarjetas créditos?	Determinar efectos sobre volumen transaccional identificando fechas específicas con mayor riesgo.	Volumen de transacciones	Incremento, disminución del riesgo de fraude
		¿Las medidas de seguridad aplicadas contienen riesgo operativo en las transacciones?	Describir los actuales puntos fuertes y débiles en los estándares o medidas de seguridad aplicadas.	Fortalezas y debilidades de los estandares aplicados	Transacciones seguras
		¿Los usuarios financieros conocen los estándares y/o medidas de seguridad de sus tarjetas de crédito?	Evaluar el conocimiento de los usuarios activos en relación a los protocolos de seguridad incorporados en su tarjeta de crédito.	Conocimiento de los protocolos de seguridad	Reducción riesgo del fraude

### 3.1.2 Esquema de Variables



### 3.1.3 Operacionalización de Variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADOR
Estandares de seguridad	Criterios para garantizar la seguridad de las actividades, procesos o medios de pagos electrónicos.	Son los procedimientos seguros para desarrollar actividades específicas comunes dentro de diferentes procesos.	estándares de seguridad como PCI DSS , Banda magnética o chip en las tarjetas ( El sistema EMV)	Control y/o revisión de Cumplimiento
Volumen de transacciones	Es el numero o monto de la transacción, realizada a través de las tarjetas de crédito.	El volumen de transacciones sirve para verificar una tendencia, determinar si la misma se sostiene en el tiempo, permite descartar o verificar situaciones que en algún momento puedan permitir el riesgo de fraude.	Sistemas de los entes financieros (Core)	Transacciones liquidadas y flotantes
Fortalezas y debilidades de los estandares aplicados	Las fortalezas y debilidades son las que permiten aprovechar las ventajas y contrarrestar sus desventajas de mejor manera.	Son los que determinan los parámetros que afectan a los diferentes indicadores al momento de definirlos como fortaleza o debilidad .	Análisis FODA de los estandares, PCI DSS , Banda magnética o chip en las tarjetas ( El sistema EMV)	Volumen de Fraudes reportados
Conocimiento de los protocolos de seguridad	Un protocolo de seguridad es un documento físico o digital de las estrategias con los pasos que se deben seguir para ejecutar medidas de protección y acciones seguras en las transacciones con medios de pagos como tarjetas de crédito.	Estas medidas te enseñan una serie de puntos que deberás ejercer para estar preparado y actuar en caso de que se presente alguna situación que ponga en riesgo tus operaciones o transacciones financieras a través de los medios de pago plásticos.	Nivel de conocimiento del Usuario Financiero	Medidas de seguridad ejecutadas por el usuario previo una transacción
Tarjeta de Crédito como medio de pago seguro	Una tarjeta de crédito, es un medio de pago emitido por un banco o una entidad financiera a favor de sus clientes (mediante la firma del oportuno contrato de tarjeta de crédito)	Son las que permite hacer uso de ella en los comercios y establecimientos que la aceptan como medio de pago, hacer extracciones en efectivo de su red cajeros automáticos y otras operaciones (recargar un móvil con tarjeta prepago, consultar el saldo de la cuenta bancaria asociada a la tarjeta, etc.).	Aceptación de HRE ( Seguro de Hurto, robo o extravío)	Tarjetas con protección y/o cobertura de fraude
Incremento, disminución del riesgo de fraude	Las tarjetas de crédito son un producto financiero que sufre más riesgos y mayor exposición que otros productos.	Existen determinadas amenazas más presentes que otras, pero que en definitiva, requieren de las mismas precauciones.	Factores de riesgo	Comercios, cajeros, y sitios web con alertas de transaccionalidad fraudulenta.
Transacciones seguras	Las transacciones seguras están respaldadas por la mayoría de los principales proveedores de transacciones electrónicas, como Visa y MasterCard. permite a los comerciantes verificar la información de la tarjeta de sus clientes sin verla, protegiendo así al cliente. La información en la tarjeta se transfiere en cambio directamente a la compañía de tarjeta de crédito para su verificación	seguridad técnica y jurídica que impida un anormal funcionamiento o una desconfianza en el medio utilizado para comerciar.	Adopción de las medidas de transacciones seguras en los comercios, cajeros, y sitios web.	Medidas preventivas ejecutadas por comercios, cajeros, y sitios web.
Reduce riesgo de fraude	Es un proceso continuo que busca proactivamente identificar y mitigar las vulnerabilidades de una organización hacia el fraude interno y externo	es la referencia a pérdidas como consecuencia de actos fraudulentos intencionales, o de robo, así como incumplimiento de leyes y políticas internas	Aplicación de políticas de mitigación de riesgo	Controles de reducción de fraude

### **3.2 Alcance, enfoque y métodos**

Se determina un alcance explicativo considerando que el mismo pretende establecer las causas del riesgo en las tarjetas de crédito como medio de pago seguro.

El tipo de investigación se enfoca en una metodología mixta realizando la recolección de datos a través de entrevista/encuesta.

### **3.3 Diseño de la Investigación**

Diseño no experimental, transeccional transversal, tomando en cuenta que la información será tomada en un solo momento, el diseño que se tome en este estudio es transversal o transaccional porque no se pueden manipular las variables. Se recolectarán datos con el propósito de definir variables y analizar su incidencia en un momento dado; en el mismo abarcar distintas personas en este caso el director de Medios de Pago y usuarios financieros de Banco Davivienda Honduras.

#### **3.3.1 Población**

La población se extrae de la cartera de clientes de tarjeta de crédito mercadeable a nivel nacional de Banco Davivienda.

Total, cartera de clientes mercadeable: 35,365

#### **3.3.2 Muestra**

Se consultará a experto en el tema, director de Banco Davivienda. Esta técnica de muestreo es un proceso que nos permite tomar un conjunto de datos obtenidos con comportamientos que se supone aleatorio.

En la muestra se consideran grupos de la población extractos, el interés es comparar resultados entre segmentos, grupos de la población.

Para realizar el trabajo de investigación será necesaria una muestra de 380 usuarios que

utilizan Tarjeta de Crédito.

Cálculo de la muestra

$N =$  tamaño de la población 35,365

$NC =$  Nivel de confianza, 95%

$P =$  probabilidad de éxito, o proporción esperada 50%

$ME =$  Margen de Error 5%;

$n^*=591$

$TNR (10\%)= 380 \times 10\%=38$

$n^*+TNR=418$

**MARGEN DE ERROR MÁXIMO ADMITIDO**  
**TAMAÑO DE LA POBLACIÓN**

5.0%
35,365

Tamaño para un nivel de confianza del 95% .....	380
Tamaño para un nivel de confianza del 97% .....	465
Tamaño para un nivel de confianza del 99% .....	653

(Granada, s.f.)

### **3.3.3 Unidad de Análisis**

Clientes de Banco Davivienda que mantienen activa una tarjeta de crédito y director de medios de pago.

### **3.4 Técnicas, instrumentos y procedimientos aplicados**

#### **3.4.1 Técnicas**

En el pilotaje de la investigación se realizaron 2 técnicas para evaluar el diseño:

1. Entrevista experta en el tema
2. Encuesta: Aplicada a clientes de Banco Davivienda que poseen una tarjeta de crédito.

#### **3.4.2 Procedimientos aplicados**

Entrevista se aplica al director de Medios de pago de Banco Davivienda con el fin de tener un conocimiento más amplio en el tema mediante una conversación directa, dicha técnica busca obtener el discurso en forma natural del entrevistado, su mundo de vida en la experiencia del tema.

Encuesta se llevó a cabo a través de la aplicación de un formulario de google instrumento que contiene preguntas abiertas, cerradas y selección múltiple, a usuarios financieros que utilizan Tarjeta de Crédito.

### **3.5 Fuentes de Información**

#### **3.5.1 Fuentes Primarias**

Información de registro de clientes y/o cartera mercadeable de tarjeta de crédito suministrada por Banco Davivienda.

Información financiera oficial reportada a través de la CNBS.

#### **3.5.2 Fuentes Secundarias**

Para enriquecer dicha investigación se consultaron informes, sitios web, artículos de revista y fuentes bibliográficas.

## **CAPÍTULO IV. RESULTADOS Y ANÁLISIS**

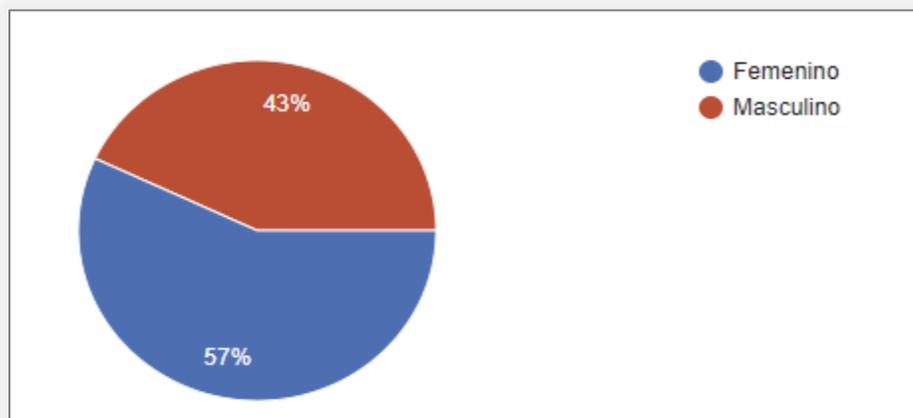
### **4.1 Análisis de resultados**

Se realizó el correspondiente análisis de las encuestas aplicadas, el total de las mismas estaban orientadas a evaluar el conocimiento en relación a los estándares de seguridad de las tarjetas de crédito de los usuarios financieros de Banco Davivienda en la ciudad de Tegucigalpa, cuya finalidad es determinar si conocen las medidas de seguridad para utilizar estos medios de pago con la precaución para mitigar la vulnerabilidad de los delitos financieros generados por el uso del conocido dinero plástico.

La misma permite conocer patrones de uso y canales de comunicación más persuasivos para desarrollar las diferentes estrategias que permitirán la formación del usuario financiero a través de la debida instrucción e información sobre el uso y las ventajas de estos medios de pago (Tarjetas de crédito) a través de los canales de comunicación con mayor efectividad y apreciación por el usuario.

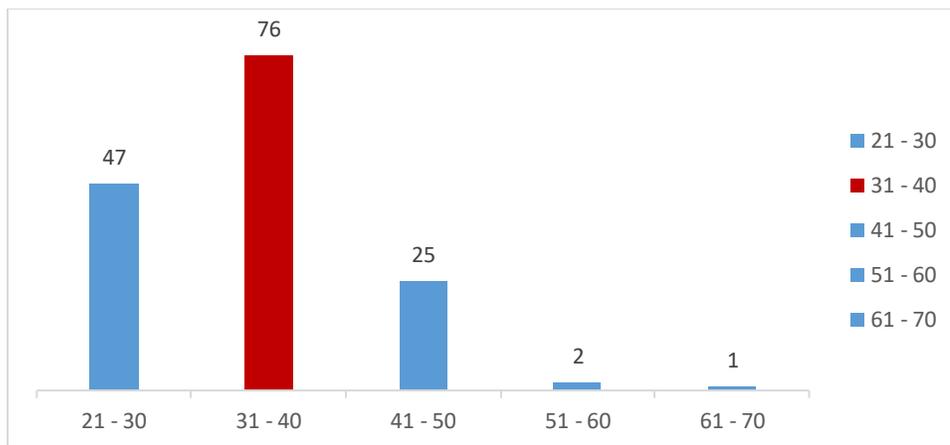
#### **4.1.1 Resultados obtenidos de las encuestas**

**Gráfico 4.1: Genero de los encuestados**



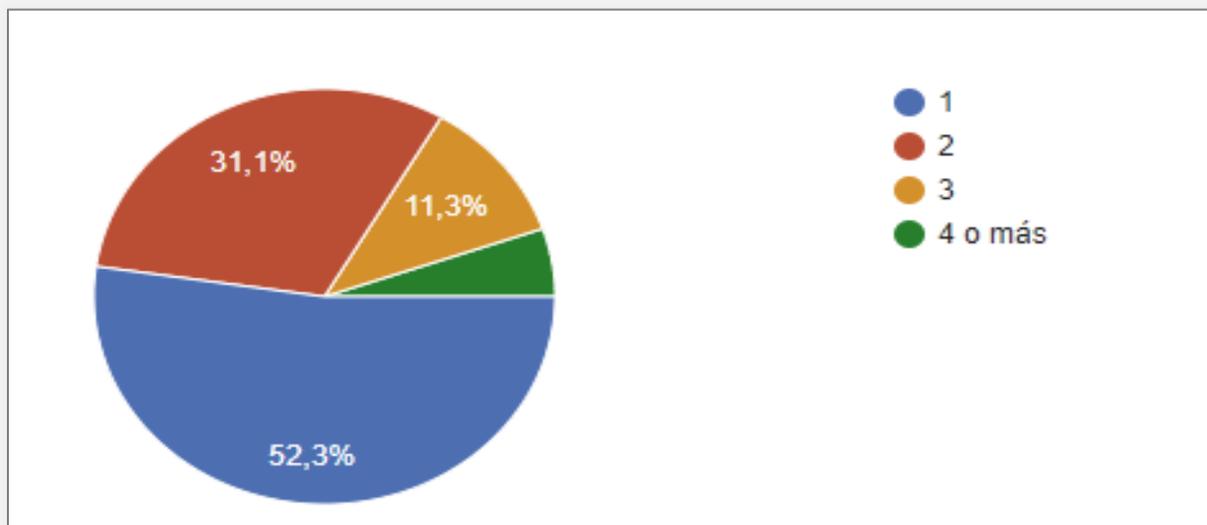
Se muestra en el grafico que antecede del total de los usuarios financieros de tarjeta de crédito encuestados predomina el género femenino con un 57% y el género masculino representa el 43%.

**Gráfico 4.2: Edades de los encuestados**



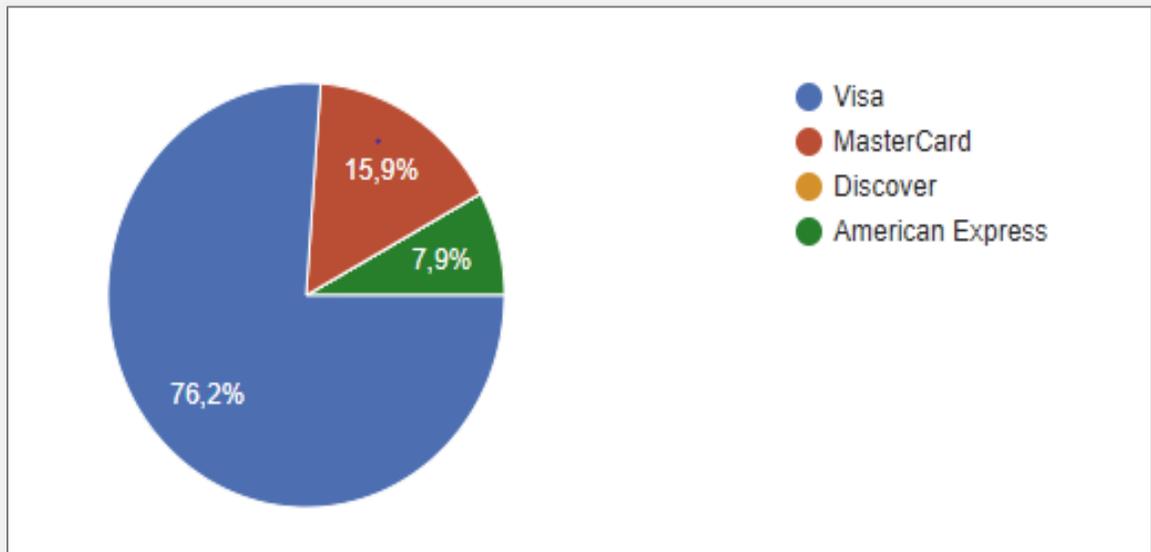
En esta gráfica se determina el promedio de edad de los usuarios de tarjeta de Crédito, estableciendo que el 82% de los encuestados predominan en un rango de edad de 21 a 40 años; y el 18% figura en edad de 41 a 70 años, denotando que los usuarios se concentran en las generaciones más sensibilizadas por los retos económicos, este nicho de mercado es favorable para la adopción de herramientas digitales con la debida diligencia y mitigación de riesgo, permitiendo a la organización un acelerado crecimiento en el mundo tecnológico.

**Pregunta 1.- Cuenta con tarjetas de crédito? ¿Cuántas?**



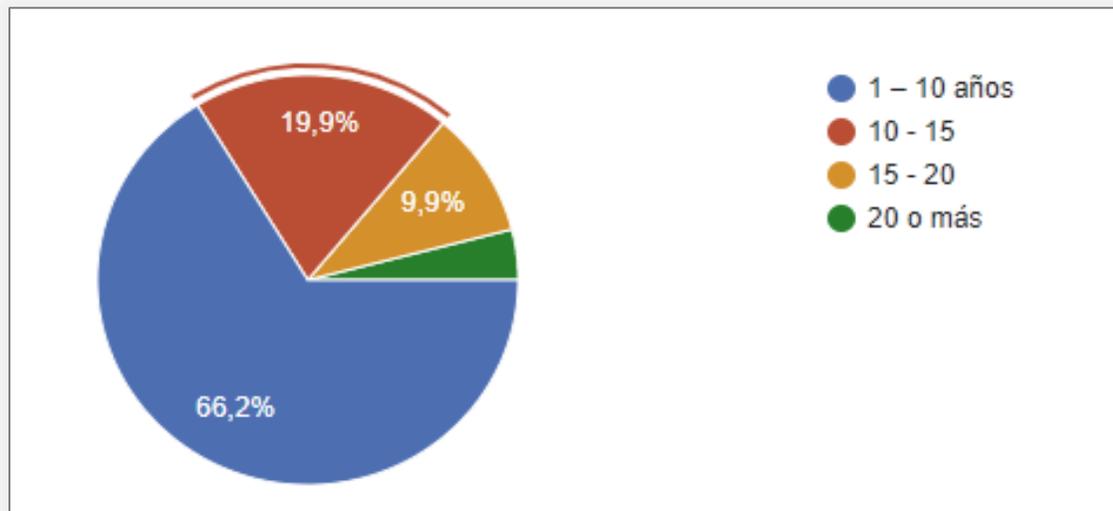
El 52.3% de los encuestados indicaron que poseen una tarjeta de crédito, cabe destacar que el 47.7% mantiene más de una tarjeta lo que denota la evolución de este medio de pago ha cobrado vital importancia en los últimos años, generando un cambio en los patrones de pago a través de dinero plástico.

**Pregunta 2.-** Si su respuesta es afirmativa que tipo de tarjeta posee?



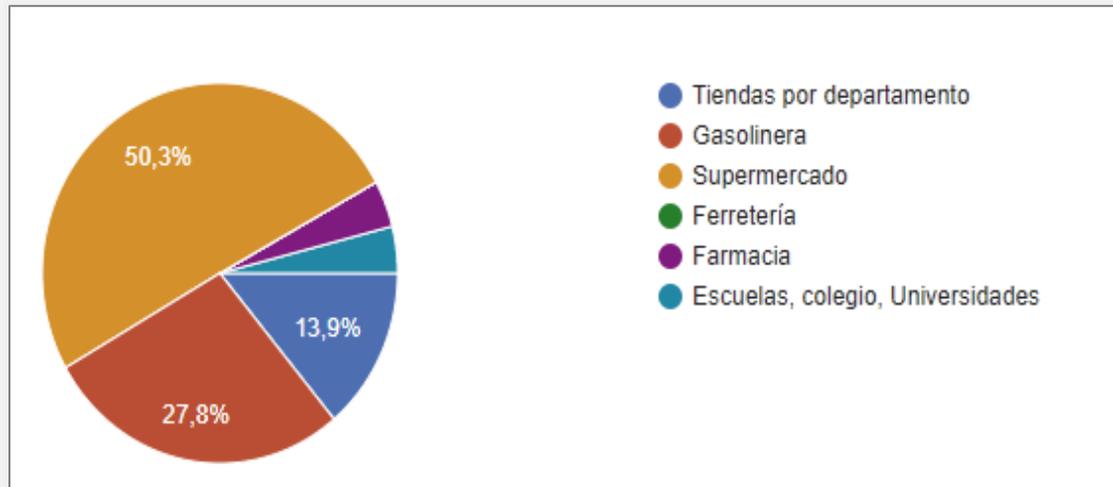
Prevalece en los resultados la marca Visa, el 76.2% nos indican que poseen una tarjeta con dicha marca, sin embargo, denotamos que MasterCard representa el 15.9% y American Express con un 7.9%, considerando dichos resultados es de relevancia la facultad que posee Visa en adherir rígidos estándares de seguridad, demandar el cumplimiento de controles a los entes financieros con los que posee una relación contractual e igual evolucionar constantemente en proveer soluciones de pago seguras.

**Pregunta 3.-** Hace cuánto tiempo posee tarjeta de crédito?



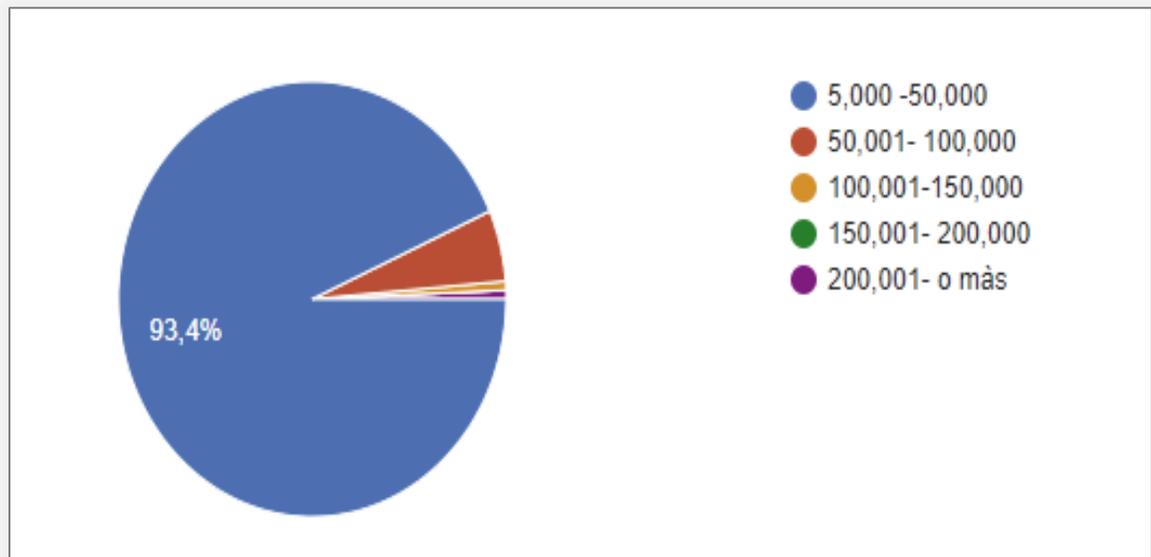
La madurez evidenciada en el uso de las tarjetas de créditos que predomina en los encuestados se encuentra en el rango de 1-10 años representando el 66.2%, cabe destacar que el 33.8% de los usuarios tiene más de 10 años de utilizar una tarjeta como medio de pago, identificada dicha experiencia e interacción con este medio de pago, permite una aceleración transicional en la evolución del mismo como medio de pago seguro.

**Pregunta 4.-** En qué comercio utiliza frecuentemente su tarjeta de crédito como medio de pago?



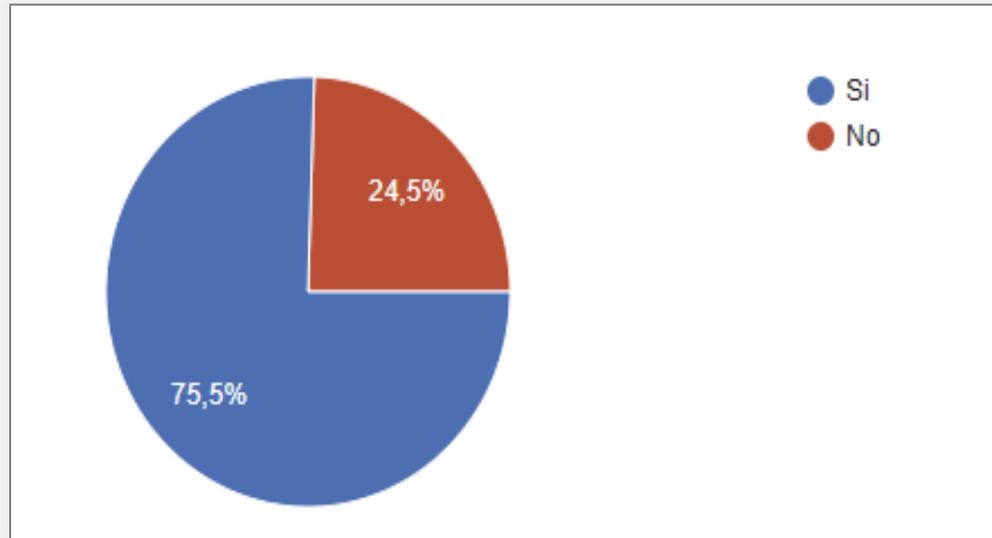
Los usuarios financieros revelan que sus consumos se orientan en supermercado representando un 50.3% seguidamente de consumo de combustible con un 27.8% y tiendas por departamentos con un 13.9%, lo que refleja que los entes financieros deben regular y supervisar con mayor frecuencia dichos establecimientos para verificar el cumplimiento de los protocolos de seguridad, certificando la aplicación de validación y/o identificación con la debida diligencia de usuarios titulares realizando sus transacciones seguras.

**Pregunta 5.-** Cuál es el valor promedio que cancela a través de su tarjeta de crédito mensualmente?



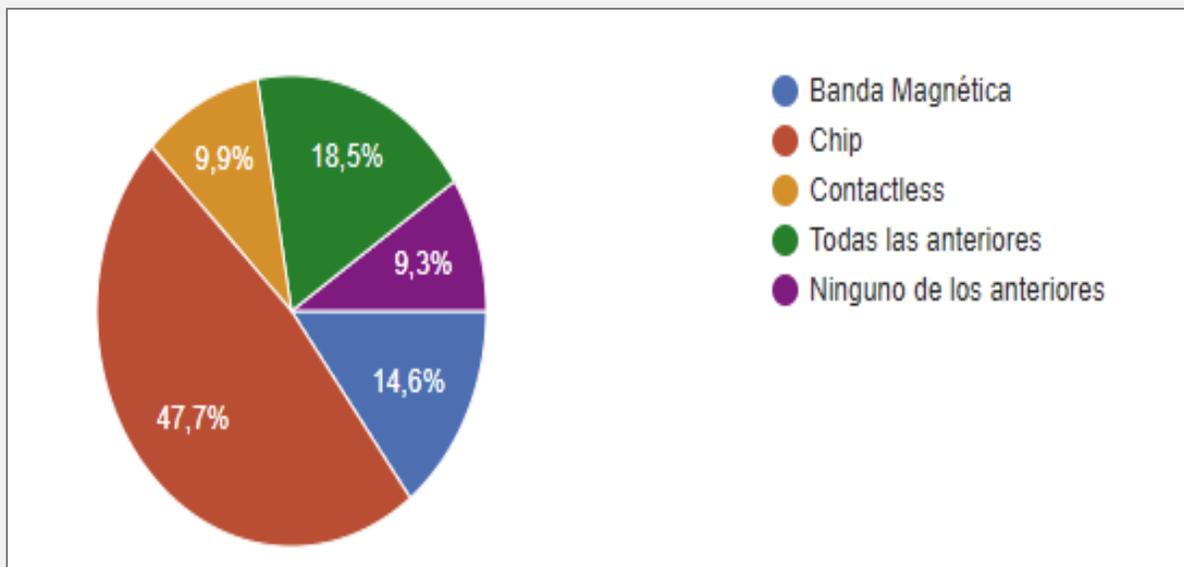
El valor promedio de las transacciones realizadas por los encuestados se concentra drásticamente en un promedio mensual de L.5,000 – L.50,000 un monto considerable para fortalecer la seguridad de dichas transacciones considerando el volumen y establecimientos identificados con el mayor tráfico orgánico de facturación.

**Pregunta 6.-** Conoce los estándares de seguridad de su tarjeta de crédito contra fraude?



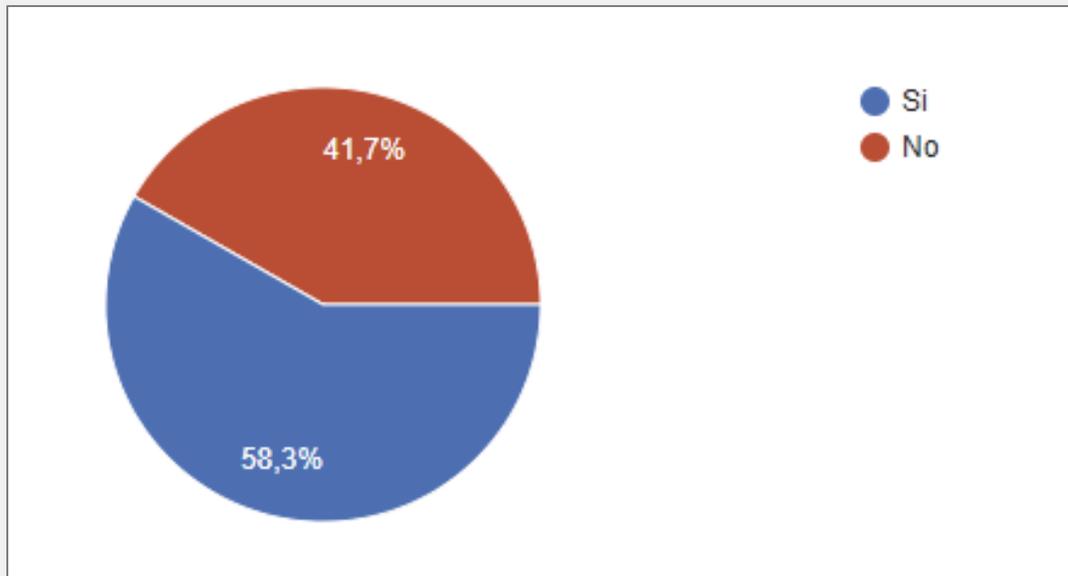
El 75.5% de los usuarios encuestados afirma conocer los estándares de seguridad de las tarjetas de crédito el 24,5% confirma el desconocer los protocolos de seguridad incorporados en las tarjetas de crédito que utilizan, considerando que dicha estadística se inclina en el conocimiento en las preguntas que preceden identificaremos cuál de los estándares incorporados prevalecen en la mente del usuario.

**Pregunta 7.-** Cuál de los siguientes estándares de seguridad usted conoce?



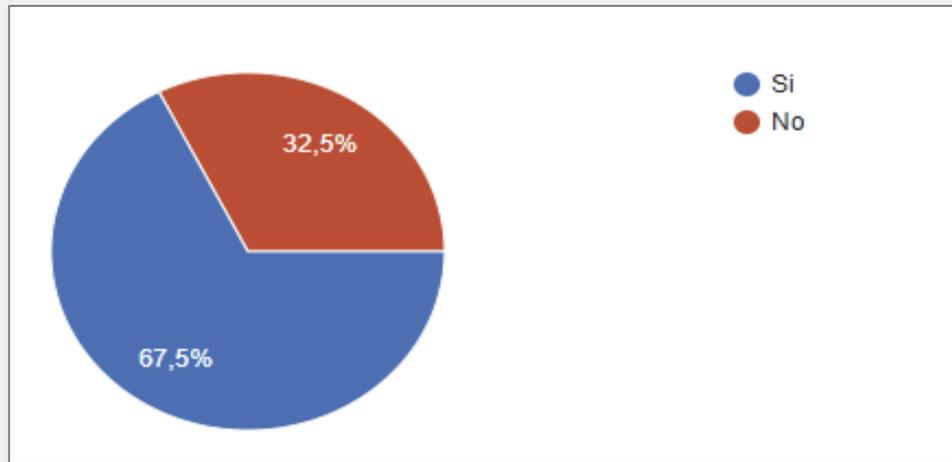
Es evidenciado que, aunque en la pregunta que antecede el 75.5% afirma conocer los estándares, al indagar cuál de los estándares conoce solo el 18.5% conoce la evolución de los mismos ya que confirma conocer todos los estándares enunciados, el 47.7% enfatiza tener conocimiento del estándar de seguridad sistema EMV (o chip). Lo que demanda fortalecer el empoderamiento y/o formación de los usuarios en la evolución de este medio de pago como seguro.

**Pregunta 8.-** Conoce para qué sirve la Banda Magnética en una Tarjeta de Crédito?



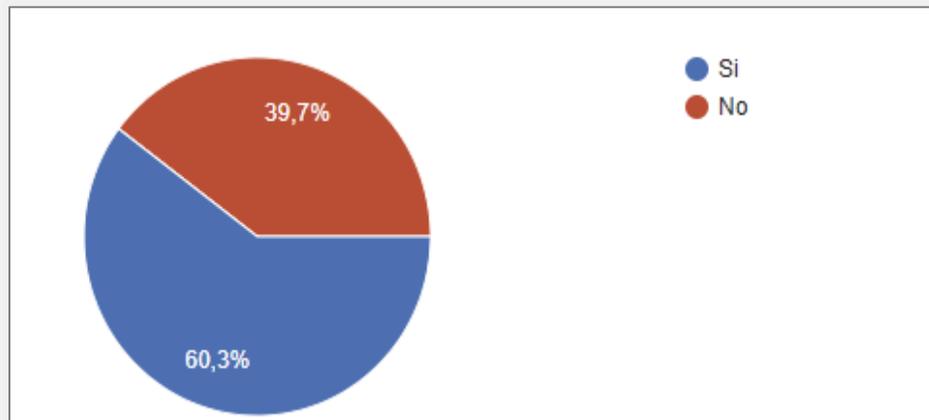
Se refleja en los resultados obtenidos que el 41.7% de los encuestados desconoce las fortalezas y/o bondades de la banda magnética como estándar de seguridad incorporado en sus tarjetas de crédito, evidenciando la vulnerabilidad presentada en dicha omisión de información, de los usuarios para realizar sus transacciones, rigiéndose con los protocolos y lineamientos de seguridad que se deben tomar en consideración al momento de realizar sus compras.

**Pregunta 9.-** Conoce para qué sirve el Chip en una Tarjeta de Crédito?



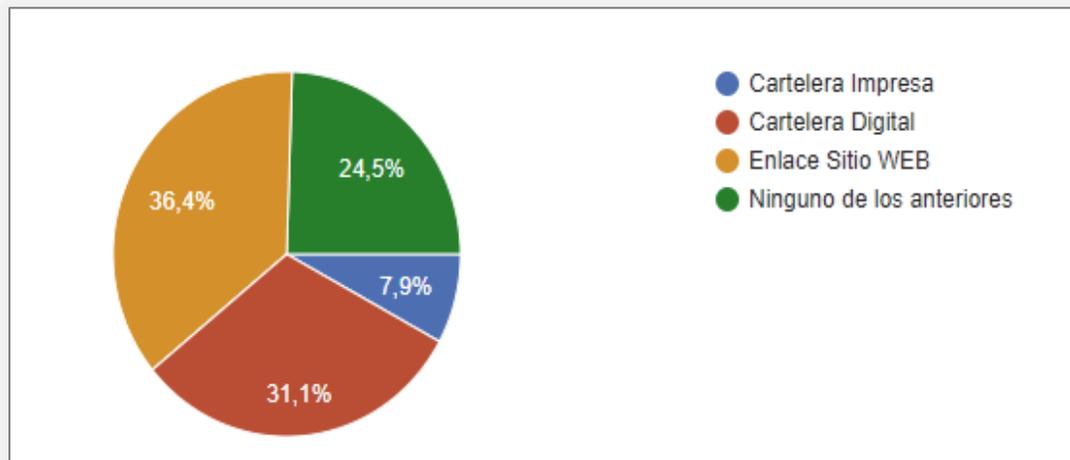
Es notable en la gráfica que el estándar de seguridad de mayor conocimiento, indicado por los usuarios financieros es el sistema EMV (o chip) cabe destacar que dicha afirmación sea influenciada por la visibilidad del mismo en su plástico y que desconozcan las ventajas inherentes en el chip como estándar de seguridad, considerando dicho resultado es necesario emplear estrategias que empoderen al usuario de las fortalezas e instruir en los procedimientos a seguir para reducir cualquier riesgo en la trazabilidad de su compra o transacción.

**Pregunta 10.-** Conoce para qué sirve el pago sin contacto (Contactless) en una Tarjeta de Crédito?



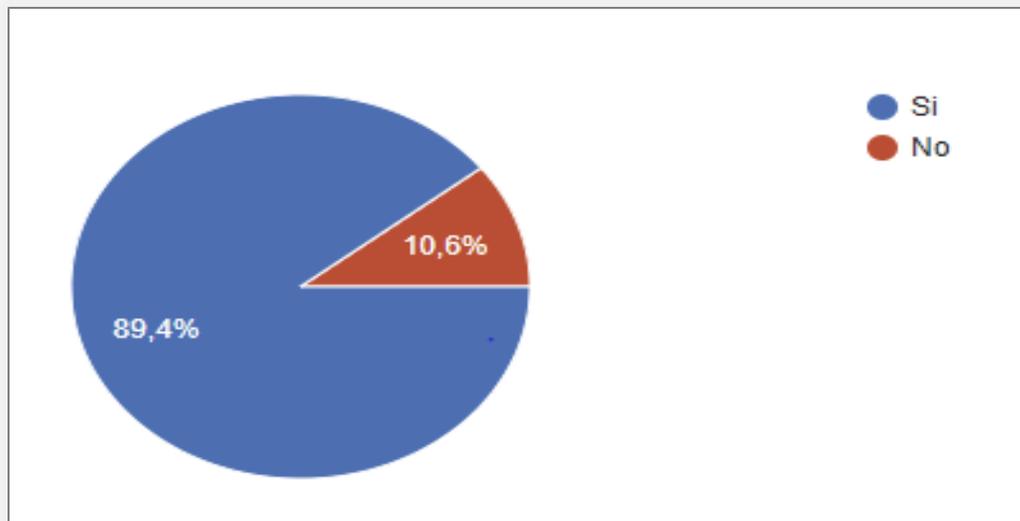
El 60.3% de los usuarios encuestados afirman conocer la funcionalidad del pago sin contacto en su tarjeta de crédito, el 39.7% representa el segmento de clientes que desconocen las ventajas del pago sin contacto como protocolo de seguridad, lo que representa un riesgo considerando que dicho protocolo es uno de los más reciente y que evidentemente hay un porcentaje sustancial que denota el desconocer su función principal para proporcionar transacciones con mayor seguridad.

**Pregunta 11.-** Si su respuesta fue afirmativa ¿Por qué tipo de medio digital los conoció?



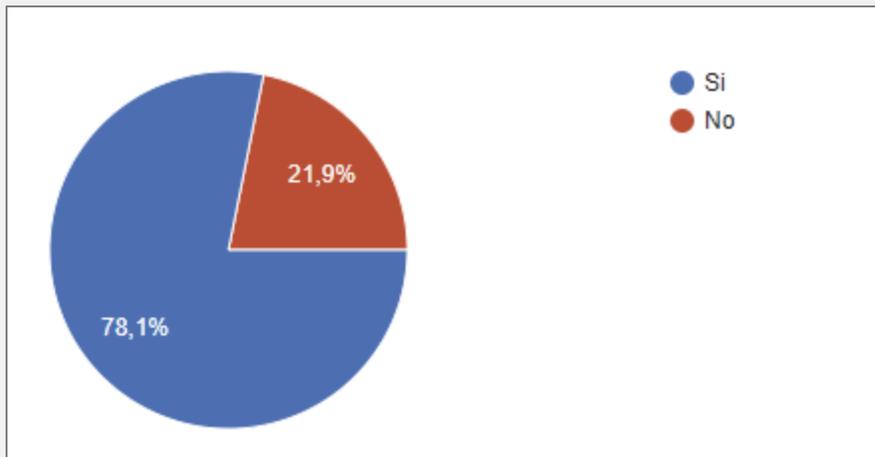
El canal de comunicación con mayor persuasión por los usuarios financieros, para formar e instruir en relación a lineamientos y protocolos de seguridad a seguir que permite reducir el riesgo de fraude en el uso de sus tarjetas de crédito, son los enlaces sitio web y canales digitales representando un 67.5%, se refleja en al extraer los resultados que la comunicación impresa esta siendo obsoleta por la reducida penetración en la audiencia de este medio, un 24.5% de los encuestados afirma no recibir información por ningún medio en mención.

**Pregunta 12.-** Considera que las tarjetas de crédito como medio de pago es segura para realizar sus transacciones?



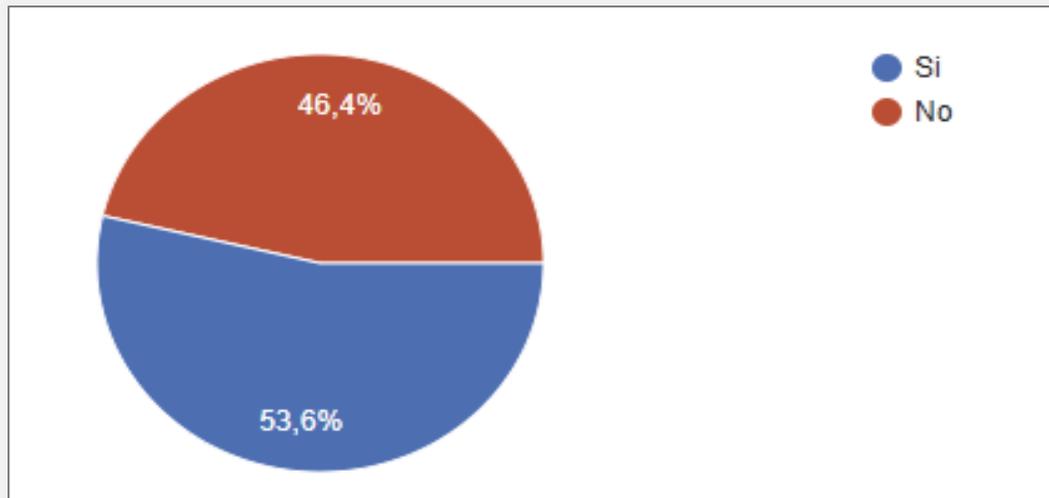
Es significativo el porcentaje de usuarios que afirman que sus tarjetas de créditos son un medio de pago seguro, cabe destacar la necesidad inherente de seguir formando al usuario en protocolos de seguridad que deben implementar en la utilización de su dinero plástico, dando apertura a transacciones seguras a través de este medio de pago, considerando que el mismo ha recobrado vital relevancia por la participación en el tráfico orgánico de facturación y consumos.

**Pregunta 12.-** Realiza revisión continua en la página web de los consumos realizados?



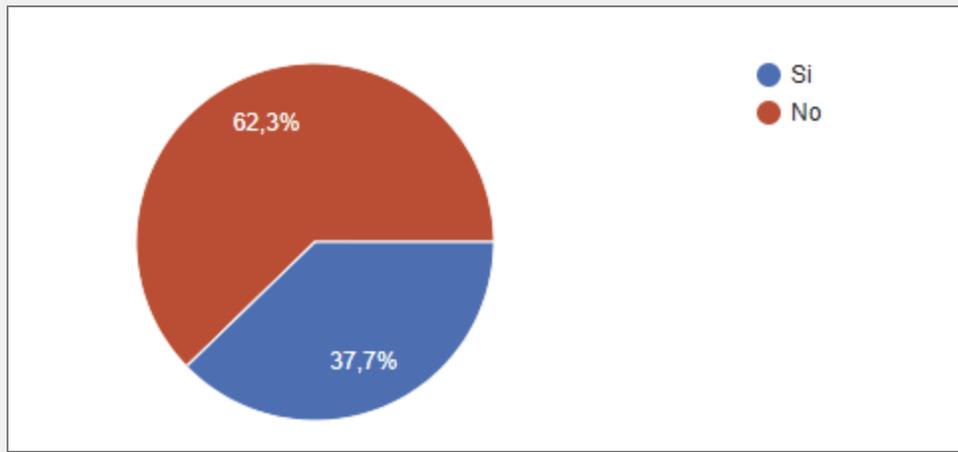
El 78.1% de los usuarios encuestado realizan certificación y/o revisiones continuas de sus consumos en la página web, el resultado reflejado nos muestra que un porcentaje sustancial de los usuarios financieros tiene interacción con las plataformas digitales disponibles, la que demanda robustecer los controles y estándares de seguridad en la navegación de los portales, páginas web y app móvil, disponibles para autogestión de los usuarios financieros.

**Pregunta 13.-** Realiza cambio periódicamente de sus contraseñas y claves en la plataforma virtual?



Los usuarios financieros encuestados expresan que periódicamente realizan cambio de sus contraseñas representando el 53.6% del total, es significativo el porcentaje de usuarios que no realizan periódicamente dicho cambio siendo este el 46.4% de los encuestados, es latente el riesgo de fraude por mantener la contraseña por un periodo extenso, ya que permite la vulnerabilidad en la identificación de dicha contraseña por los que practican el delito financiero.

**Pregunta 13.-** Como medida de seguridad registra su firma en la tarjeta de crédito?



Se confirma que el 37.7% de encuestados continúa registrando su firma en la tarjeta procedimiento que hace un tiempo relevante se omite por el riesgo de visibilidad de la firma de la titular expuesta para ser objeto de falsificación o usurpación de identidad, incrementando el riesgo de fraude en sus transacciones.

**Pregunta 14.-** ¿Para qué sirve el CVV de verificación de 3 dígitos incorporados en su tarjeta de crédito?

El 31.1% desconoce la funcionalidad de su código CVV impactando el riesgo de facilitar dichos dígitos, por falta de conocimiento expuesto hacer potenciales prospectos de fraude, por desconocer que el mismo es un único código de seguridad que permite la verificación de seguridad y es uno de los protocolos de control y checklist para certificar transacciones y/o compras en línea minimizando el riesgo de fraude.

## **4.2 Resultados obtenidos a partir de la entrevista**

### **4.2.1 Experto encuestado director de tarjeta de crédito, Banco Davivienda Ing. Fabio Tabora.**

**Pregunta 1.-** ¿Cuál ha sido la evolución de tarjetas de crédito como medio de pago?

Los emisores de tarjetas a finales de los años 1980 y 1989 nace Credomatic; en el año 1991 Aval Card, tenían un call center de autorización con seguridad pobre, porque los comercios tenían inicialmente la obligación de solicitar una identificación válida por país, que normalmente han sido las mismas hasta la fecha (identidad, licencia de conducir o carnet del seguro), las identificaciones con fotografía válidas para el país esto se prestaba mucho a que una persona que no es hondureña se robaba los números de las tarjetas de crédito y se troquelada en otro plástico y con el nombre de otra persona; normalmente el baucher que sale del aparato dice el nombre de la persona, en tiempos atrás no existía los comercios tenían una línea directa a un call center de autorización que consultaban los últimos 4 dígitos de la tarjeta, fecha de vencimiento y mantenían un sistema de autorización básicamente lo que hace el POS y les indicaba la transacción aprobada.

En este sistema se generaba bastante el fraude por el robo de información en términos de número de tarjeta de crédito, entraban a las bases de datos de los diferentes emisores y se robaban un segmento de clientes; en este punto hay un tema de seguridad en la troquelación de los plásticos existen llaves que se cargan de las marcas en las máquinas que emiten plásticos de las entidades financieras, pero en años anteriores había forma de falsificar las llaves y conseguían las máquinas con bajo costo por internet las bandas criminales.

**Pregunta 2.-** ¿Cuáles son los pasos de la evolución de tarjetas de crédito?

Se inició en el año 1990 con transacciones por comercios electrónicos lo que hacen los delincuentes robarse la información de los comercios. En el año 2015 y 2016 se presentó robo de información de millones en números de tarjetas a empresa TARGET, como Banco Davivienda también absorbió un costo por pérdida de información.

Se utilizó la banda magnética donde se robaban la información en los medios de pago utilizando Skimming que es un lector de banda magnética que su costo de adquisición no es mayor a \$10.00, lo que hacen las bandas de criminales les pagan a meseros, bomberos de gasolinera, antes el mesero del restaurante se lleva la tarjeta hasta el POS de la caja en el trayecto al momento de pasar la banda magnética el aparato lee la información y la descarga posteriormente lo envía a través de una USB para ejecutar fraudes a los usuarios.

En esta evolución también viene el tema del monitoreo que, si una cliente realizada transacciones fuera del monto totalmente diferente fuera de su comportamiento generaba alertas, las bandas de criminales se dieron cuenta y posteriormente fueron realizando compras mínimas en minutos en comercio electrónico ficticio afiliado como adquirencia. La utilización de la plancha se realizó hasta el año 2006, por las razones que había comercios electrónicos que no tenían teléfono fijo, en 2007 ya se comenzaron con las transacciones electrónicas más seguras para el banco y usuarios de los medios de pago.

Posteriormente se logró migrar al Chip para esta metodología hay una llave especial de inscripción y protocolo de comunicación entre Chip y POS, es un protocolo de seguridad seguro que por los momentos no hay forma que lo puedan copiar. El BIN local o Internacional son los primeros 6 dígitos detecta si es un BIN que está relacionado con chip por el plan de

implementación que se ejecutó con las marcas (visa, MasterCard, Etc.)

Posteriormente se realizó un ajuste con todas las marcas de tarjetas de crédito para implementar el protocolo de seguridad se unió con una compañía importante llamada Europay MasterCard Visa (EMV). Los plásticos que circulan tienen incorporado banda y chip, pero si el BIN detecta que es utilizada a través de la banda rechaza para afectación a través del chip y le solicita el POS que utilice a través del chip. Por medio de utilización de la banda pueden robarse información. El CVV código de seguridad de las marcas se utiliza para compras por internet.

En el mes de octubre del año 2019 se emigró a CONTACTLESS (transacciones de pago sin contacto) donde este lector detecta o realiza lectura de antena para enviar información a chip, hoy en día las transacciones físicas o plásticos presentes cuentan con los protocolos chip y contactless métodos seguros en el mundo de la tecnología.

En Europa y Estados Unidos el medio de pago lo tienen en su aparato móvil. Anteriormente se verificaban transacciones manualmente por montos y actualmente se ha logrado avanzar para el monitoreo con un sistema neural mismo que está parametrizado para los nuevos comportamientos de los clientes, el sistema genera alertas para los clientes que realizan transacciones inusuales, los analistas de prevención de fraude verifican básicamente lo que el sistema les genera.

Toda entidad financiera deberá migrar a tokenización significa que como emisor tengo un BIN específico y lo tengo con token esto significa que, como cliente inserto mi tarjeta en un comercio electrónico, el comercio le pregunta al emisor y si el emisor está tokenizado no me devuelve mi número de tarjeta al momento de la compra, el emisor le va devolver al comercio un número de token asociado a la cuenta del cliente con esta nueva tecnología se evitan los fraudes en medios electrónicos.

Los plásticos actuales cuentan con incorporación: contactless, número de tarjeta, nombre, banda, CVV; hace falta ir migrando a token para evitar robo de información, se requiere mantener estas incorporaciones para asegurar las transacciones de los clientes por si algún país no cuenta con las características actuales de Chip, banda, contactless.

No existe una regulación, pero toda Institución debe cumplir con los manuales operativos en los contratos firmados con la marca para evitar: penalizaciones, fraude, cancelación de licencia por uso de marca.

Como operadores debemos de cumplir con todas las regulaciones establecidas por la marca, los procesadores que se dedican al procesamiento de medios de pagos electrónico también tienen contrato con las marcas dado que les otorgan autorización para procesar transacciones de los clientes, los bancos y procesadores mantienen obligación contractual con las marcas.

**Pregunta 3.-** ¿En relación a la vulnerabilidad de las transacciones impacta al ente financiero o usuario?

Internamente los clientes llevan la posibilidad de ganar y no asumir los costos por transacciones en disputas. En Davivienda y otros bancos cuenta con envío de SMS y correos electrónicos por alertas de transacciones realizadas, los clientes tienen la obligación de solicitar bloqueo de sus tarjetas por transacciones no reconocidas.

Los riesgos operativos se trasladan a la compañía de seguros para asumir estos imprevistos, según la ley de tarjeta de crédito los fraudes electrónicos son atribuible al emisor por lo que las instituciones financieras deberán tener su cartera asegurada, todo reclamo de consumo no reconocido ingresa a una unidad de análisis (marca, arbitraje) para verificar las transacciones presentadas de no reconocimiento por parte del cliente.

En caso que los clientes no mantengan la cobertura y la transacción sea realizada por una tercera persona el banco absorbe el costo como riesgo operativo para este tipo de imprevistos es menos del 1% en comparación a nuestra cartera de crédito y estos casos están asegurados con una compañía de seguros.

**Pregunta 4.-** ¿Considera que los estándares de seguridad actuales tienen una cobertura optima?

Si, pero falta realizar la migración a modalidad BIN token, las bandas de delincuentes tendrán más difícil el tema de robo de información.

**Pregunta 5.-** ¿Considera que, si se empodera el conocimiento de los usuarios en relación a los estándares de las tarjetas de crédito, mitigaría el riesgo para las entidades financieras?

Sí, a medida la tecnología avanza los usuarios financieros van aprendiendo, cabe mencionar que hace falta la educación de los usuarios, algunos bancos han enviado campaña sobre temas de seguridad, hay un tema de falta de interés por parte del usuario, no lee la información sobre tema de seguridad.

**Pregunta 6.-** ¿Cuál es el medio más óptimo para comunicar a los clientes?

Todo se está emigrando a móvil y redes sociales, se deberá desarrollar más canales móviles (APP), el tema digital más obligatorio, uno de los retos es bancarizar a la población para apertura de productos financieros (tarjeta de crédito, cuenta de ahorro, prestamos). Todo comercio se está adaptando a la metodología de recibir sus pagos a través de un POS por tema de seguridad.

## **CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES**

### **5.1 Conclusiones**

1. Se identifica una clara evolución en los estándares de seguridad comenzando desde la banda magnética, seguido del sistema EMV y/o chip, posterior se migro al sistema de contactless y en la actualidad a la tokenización, lo que demanda a los entes financieros robustecer y adoptar los controles y estándares de seguridad más actualizados.
2. El valor promedio de las transacciones realizadas por los usuarios se concentra drásticamente en un promedio mensual de L.5,000 – L.50,000, los meses y días de mayor riesgo por su volumen transaccional se centran en junio, julio, octubre y diciembre, y los días 15-17 y 30-1 de cada mes.
3. Dicha investigación permitió el comportamiento de compra, revelando que sus consumos se orientan en supermercados, seguidamente de consumo de combustible y tiendas por departamento, las preferencias del canal de comunicación evidenciando tener mayor persuasión los enlaces en sitio web y canales digitales.
4. Los usuarios de tarjeta de crédito evidencian que desconocen los estándares y/o medidas de seguridad incorporadas en la misma, afirmando solo el 18.5% conocer la evolución de los mismos siendo latente los posibles fraudes y el riesgo operativo para los entes financieros.

## **5.2 Recomendaciones**

1. Ofrecer experiencias seguras mejoradas con la adopción de estrategia de adquisición, activación mediante un programa de aceleración que utilice los estándares innovadores o más recientes que permiten transacciones más seguras, brindando una propuesta de valor por la incorporación de mejores prácticas, demandando incorporar el más reciente estándar de seguridad que es la tokenización.
2. A medida que los usuarios viven más experiencias de pago sin contacto, surge la imperiosa necesidad de ofrecer soluciones de pagos con dinero plástico, para garantizar experiencias más rápidas, seguras y convenientes, lo que, demanda implementar controles de seguridad, aplicación de alertas y robustecer el ente de monitoreo, empoderando de ejecutar controles más restringido, en transacciones con volúmenes sustanciales, meses y días con mayor riesgo.
3. Redefinir la combinación de canales para la efectiva comunicación de protocolos y/o medidas de seguridad que incluyan información holística de sus tarjetas de crédito, lo virtual es prioridad como estrategia de reformulación de dichos canales, es necesario migrar por completo la interacción y comunicación con el usuario a un entorno digital empleando, la evolución omnicanal, a través de los enlaces web identificados como el canal de mayor percepción.
4. Estrategias de empoderamiento y educación financiera para el usuario en relación a la adecuada utilización de este medio con la aplicación de medidas de contención de fraude y/o riesgo en sus transacciones, describiendo las partes de la misma su función y riesgo de divulgación, para ello, incorporando las políticas de seguridad para aceptación a través checkbox por el usuario en la página Web y App móvil, la

utilización de cartelera digital que contenga SMS HTML, llamadas IVR, empoderar a través de campañas informativas y formativas el cliente interno y/o funcionarios para salvar guardar datos e información sensitivos de los clientes, utilizar canales digitales de la organización Workplace e Informador oficial de la institución.

## **CAPITULO VI. APLICABILIDAD**

### **6.1 Introducción**

En el presente capítulo se enuncia la propuesta que permitirá la ejecutoria de acciones específicas para empoderar a los usuarios financieros de tarjeta de crédito en relación a los estándares y/o protocolos de seguridad incorporados en sus tarjetas de crédito permitiendo la reducción del riesgo de fraude y/o delito financiero en sus transacciones a través de este medio de pago.

### **6.2 Nombre de la propuesta**

Versión 1 Manual instructivo Medidas de seguridad de tarjeta de crédito.

### **6.3 Justificación de la propuesta**

El objetivo de esta investigación que guio los hallazgos de este manual fue la de evaluar el conocimiento de los usuarios financieros en relación a los estándares y/o protocolos de seguridad incorporados en sus tarjetas de crédito, por lo antes mencionado los resultados que se obtuvieron de esta investigación constituye un aporte significativo para las entidades financieras ya que provee información base del conocimiento de los usuarios financieros del producto otorgado, sus preferencias de consumo, canales de comunicación con mayor persuasión, marca que predomina, así como incentivar la adquisición de las tarjetas de crédito para aquellos usuarios financieros en potencia, interesados en realizar transacciones ágiles y seguras profundizando el tema de la seguridad en las transacciones a través de este medio de pago.

Los resultados derivan directamente de la evidencia recopilada la que permite implementar diferentes estrategias con mayor amplitud, y una ejecutoria efectiva por la identificación de los canales de comunicación de mayor persuasión, para empoderar a los usuarios de tarjeta de crédito en relación a los estándares y protocolos de seguridad, incorporados en la misma, que deben tomar

en consideración en las transacciones que realicen, mitigando el riesgo inherente de fraude y/o delito financiero.

Se enuncian los estándares y medidas de seguridad que se vuelven una mejora continua por el rubro financiero, demandando ser pioneros de procesos tecnológicos que se innovan para reducir riesgos y hacer más expedita la experiencia del producto y/o servicio que proporcionan.

#### **6.4 Alcance de la propuesta**

Desarrollar un manual guía y/o instructivo que contiene estrategias de comunicación para empoderar a los usuarios financieros holísticamente en relación a las medidas de seguridad de sus tarjetas de crédito, formándoles desde conocer la funcionalidad de las partes principales de su tarjeta y protocolos de seguridad que deben implementar, así como proporcionar información relevante para la industria financiera que comercializa dicho producto, la evolución de las medidas de seguridad como un ciclo de transición constante, que siempre admite mejoras cuyo propósito es reducir y/o mitigar el riesgo y pérdida operativa por el delito financiero inherente.

##### **6.4.1 Objetivos de la Implementación**

1. Formar e instruir al usuario financiero en relación al uso efectivo de sus tarjetas de crédito, a través de canales de comunicación de mayor captación para dicha audiencia.
2. Describir los actuales puntos fuertes y débiles en los estándares y/o protocolos de seguridad aplicados.
3. Identificar los rubros de mayor facturación y tráfico orgánico, para robustecer las medidas y/o protocolos de seguridad en sus transacciones.
4. Enumerar fechas y comercios específicos de mayor riesgo por el volumen transaccional.
5. Detallar la evolución de los estándares de seguridad aplicados en la industria a nivel global para la adopción en incorporación en el rubro financiero local.

## **6.5 Descripción y desarrollo de la propuesta**

Desarrollar las estrategias de empoderamiento de los usuarios con contenido actualizado, que incluya conocimiento holístico de sus tarjetas y medidas que deben adoptar al realizar sus transacciones a través de los medios de comunicación de mayor penetración destacados en la investigación.

Proporcionar los estándares y medidas de seguridad que se vuelven una mejora continua por el rubro financiero, demandando ser pioneros de procesos tecnológicos que se innovan para reducir riesgos y hacer más expedita la experiencia del producto y/o servicio que proporcionan.

<b>Principales Amenazas</b>	Actividad de Prevención
<ul style="list-style-type: none"><li>• <b>Red segura</b></li></ul> <p><b>_Ejecución de transacciones seguras.</b></p>          <p><b>_Protección de la información</b></p>	<p>_Ejecución de transacciones seguras.</p> <p>_PIN personal único.</p> <p>_ATM (estación de seguridad)</p> <p>_Canal Web (página oficial).</p> <p>_Módulos seguros para minimizar los fraudes.</p>  <p>_ Incorporación de la evolución de estándares de seguridad, que salvaguarda</p>

<p><b>_Medida de control de acceso</b></p>	<p>dicha información.</p> <p>_Redes y sistemas seguros.</p> <p>Identificación única a cada usuario. (ID y/o usuario personalizado)</p> <p>_Autorización del usuario a través de sus contraseñas.</p> <p>_ Autenticación del usuario financiero a través de biometría.</p> <p>_Firma Digital del usuario.</p>
<p><b>_Monitoreo y prueba de las redes</b></p>	<p>Revisión y permiso del usuario (pantalla de autorización)</p> <p>_ Procesamiento de la información con registro automático de la trazabilidad en el sistema.</p> <p>Inclusión de herramientas de seguridad informática.</p> <p>_Segmentación de la red _Escaneos de</p>



	<p>_Bloqueo preventivo mecanismo de seguridad que identifica patrones de comportamiento en sus consumos inusual.</p> <p>_Bloqueo preventivo de facturación en comercios identificados con porcentajes significativos de fraude.</p> <p><b>Dia, mes posible con riesgo de fraude.</b></p> <p>_ Mes: junio, julio, octubre y diciembre, por la estacionalidad e incremento en volumen transaccional.</p> <p>_Dia: 15-17 y 30-1 de cada mes.</p>
--	---

### 6.5.1 Plan de Acción empoderar usuario de tarjeta de crédito

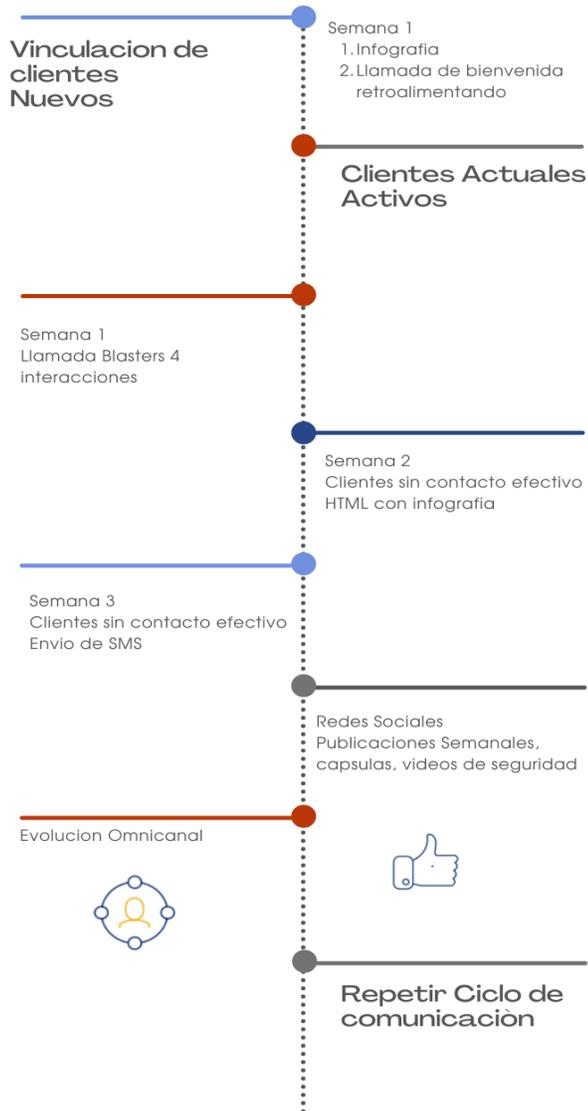
Estrategia	Descripción	Acciones realizar	Responsable
<b>Empoderar de Usuario Tarjeta Crédito</b>	<b>*Proceso:</b> <b>Entrega:</b> Kit de entrega de tarjeta.	- Anexar infografía con la descripción del protocolo de seguridad que incluya descripción de las partes de su tarjeta y funcionalidad.	-Unidad de Producto Medios de pago - Mercadeo - Operaciones
	Actualización del Proceso de enrolamiento en el App y pagina Web	-Inclusión en la interfaz de inicio, para aceptación, las políticas de seguridad a través checkbox por el usuario.	- IT - Gestión Integral de Riesgo
	<b>*Llamadas:</b> Programación de llamadas clientes actuales para formación en relación a los estándares y protocolos de seguridad	-Elaboración de script para blasters - Aprobación de script y grabación de llamadas. -Campaña blaster con una saturación de 4 intentos al día, intervalos de dos horas.	- Producto Medios de pago - Mercadeo - Canales de venta Medios de pago
	<b>*Mensajitos:</b> Seguimiento a usuarios financieros sin contacto en las interacciones con los canales de comunicación que anteceden.	SMS landing “enrolamiento App Móvil” HTML a través de correo, herramientas de soporte eloqua	- Producto Medios de pago - Mercadeo - Canales de venta Medios de pago

**6.5.2 Plan de Acción certificación y supervisor del riesgo por comercios con mayor volumen transaccional**

Estrategia	Descripción	Acciones realizar	Responsable
Certificación y supervisión del riesgo	<p><b>*Comercios:</b>  <b>Supermercados, gasolineras, tiendas por departamento.</b> Comercios infringiendo protocolos de certificación del titular de la tarjeta</p> <p><b>Marca de Tarjeta de Crédito:</b></p> <ol style="list-style-type: none"> <li>1. Visa</li> <li>2. MasterCard</li> <li>3. American Express</li> </ol>	<ul style="list-style-type: none"> <li>- Clausula contractual cumplimiento protocolo de seguridad.</li> <li>- Solicitud de documento de identificación ID</li> </ul>	<ul style="list-style-type: none"> <li>-Unidad de Producto Medios de pago.</li> </ul>
		<ul style="list-style-type: none"> <li>- Las Marcas de Tarjetas tienen una oportunidad histórica para activar sus recursos brindando experiencias seguras migrando a un modelo de acceso universal a los pagos digitales con máximos estándares de seguridad.</li> </ul>	<ul style="list-style-type: none"> <li>- Productos Medios de Pago</li> <li>- Gestión Integral de Riesgo</li> <li>- IT</li> </ul>
	<p><b>*Meses y Días:</b>            Activación de control y alertas de volumen transaccional</p>	<ul style="list-style-type: none"> <li>- Mes: junio, julio, octubre y diciembre, por la estacionalidad e incremento en volumen transaccional</li> <li>_Dia: 15-17 y 30-1 de cada mes.</li> </ul>	<ul style="list-style-type: none"> <li>-Seguridad de la Información</li> <li>- Gestión Integral de Riesgo</li> <li>- Monitoreo</li> </ul>

## 6.6 Cronograma de actividades

# CRONOGRAMA DE Actividades



### **6.6.1 Justificación del presupuesto**

El presupuesto es representado en términos costo-beneficio el cual contribuye para la incorporación de la infografía con contenido de protocolos de seguridad y descripción de las partes que conforma las tarjetas de crédito para salvaguardar los datos sensitivos, en la interfaz del App para aceptación a través checkbox por el usuario y la formación de clientes en la interacción segura en sus plataformas digitales, este tipo de inversión permitirá mitigar y reducir el riesgo de fraude y perdidas monetarias, brindando soluciones optimas expeditas y seguras en las transacciones, con el desarrollo de las estrategias de empoderamiento de los usuarios financieros y acciones descritas en el presente "Manual instructivo Medidas de seguridad de tarjeta de crédito"

<b>Componente</b>	<b>Presupuesto por implementación de los protocolos de seguridad en el APP</b>		<b>Presupuesto por implementación de los protocolos de seguridad en el APP</b>	
	<b>Costo X HR</b>	<b>Costo total</b>	<b>Soporte/ Post implementación</b>	<b>Soporte/ Post implementación</b>
<b>BUS / SCN</b>	\$29 x 160hr	\$4,640.00	50%	\$2,320.00
<b>Todo 1</b>	\$29 x 160hr	\$4,640.00	50%	\$2,320.00
<b>Infraestructura</b>	\$29 x80hr	\$2,320.00	0	0
<b>Total</b>	<b>400hr</b>	<b>\$11,600.00</b>	<b>50%</b>	<b>\$4,640.00</b>
	<b>\$11,600.00</b>		<b>\$16,240.00</b>	

En la tabla subsiguiente se detalla la inversión en la evolución omnicanal a través de llamadas blasters y SMS que contribuyen significativamente en la educación y/o formación del usuario financiero en relación a los estándares de seguridad incorporados en su tarjeta de crédito.

GVM	Presupuesto llamadas blasters, SMS		Presupuesto llamadas blasters, SMS	
	Costo X unidad	Costo X llamada contestada	% de contacto 80%	Soporte/ Post implementación
IVR	\$0.19	\$0.19	28,292	\$5,375.00
SMS	\$0.07	\$0.07	7,073	\$495.11
Total			35,365	\$5,870.00
			\$5,870.00	

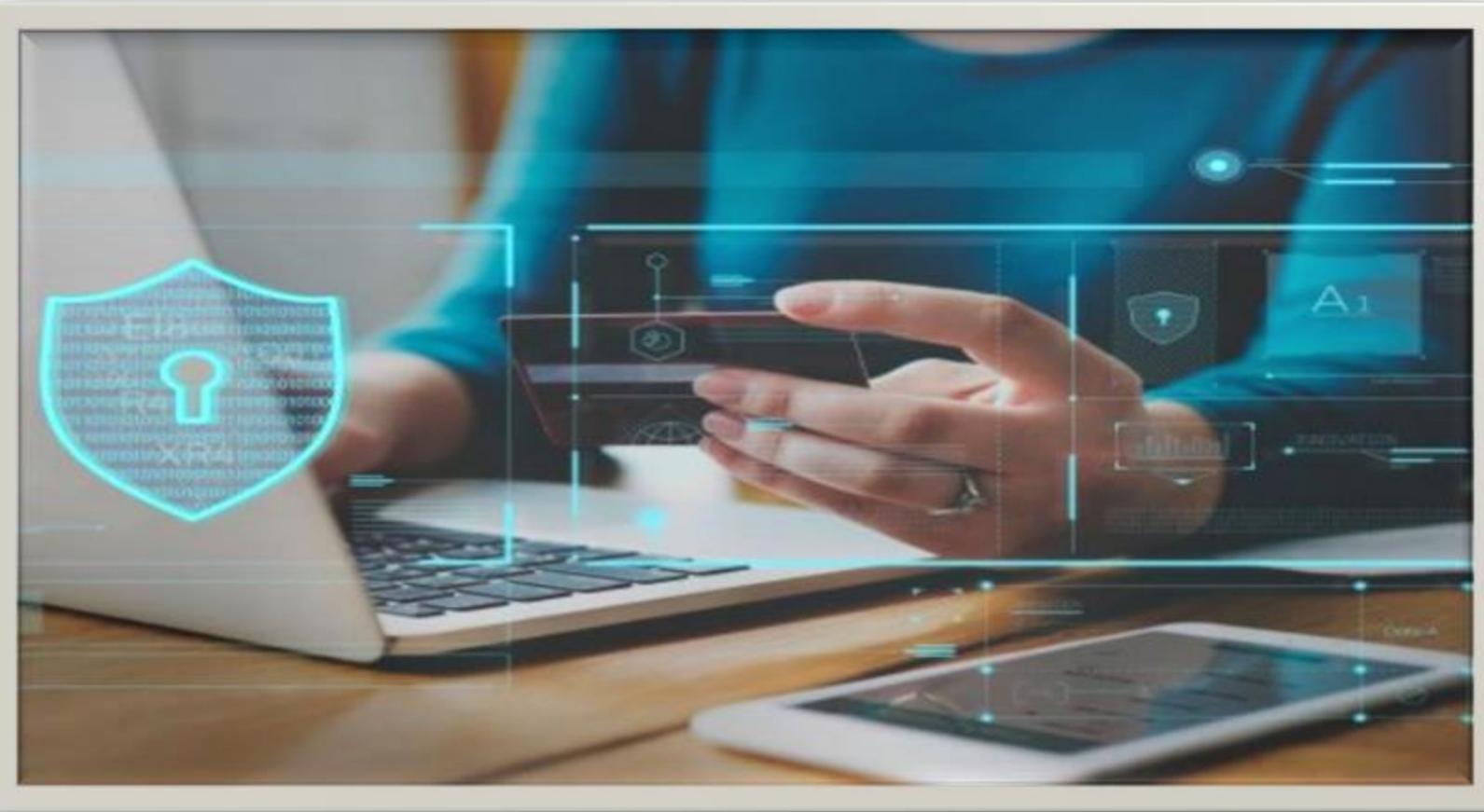
## 6.7 Tabla de concordancia

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título Investigación	Objetivo General	Objetivos Específicos	Metodologías de sustento	Variables	Poblaciones	Técnicas	Conclusiones	Nombre propuesta	Objetivos propuesta
Evolución de las tarjetas de Crédito como medio de pago seguro	Determinar acciones focalizadas en la formación e instrucción del usuario en relación al uso efectivo de las tarjetas, mitigando riesgos y fortaleciendo la utilización de las mismas como un medio de pago seguro.	1. Identificar estándares de seguridad aplicados en la industria de los medios de pago para las tarjetas de crédito.	1. Proceso de investigación participativo con la población, se realizó la recopilación secundaria, observación directa y la aplicación de encuestas dirigidas a los diferentes grupos ocupacionales.	Conocimiento de los usuarios activos	La población se extrae de la cartera de clientes de tarjeta de crédito mercadeable a nivel nacional de Banco Davivienda. Total, Cartera 35,365	La técnica implementada fue mixta: 1. Encuesta 2. Entrevista	1. Los usuarios financieros evidencian que desconocen los estándares y/o medidas de seguridad incorporadas en la misma, afirmando solo el 18.5% conocer la evolución de los mismos siendo latente los posibles fraudes y el riesgo operativo para los entes financieros.	Versión 1 Manual instructivo Medidas de seguridad de tarjeta de crédito.	1. Formar e instruir al usuario financiero en relación al uso efectivo de sus tarjetas de crédito, a través de canales de comunicación de mayor captación para dicha audiencia.
		2. Determinar efectos sobre volumen transaccional identificando fechas específicas con mayor riesgo.	2. Estudio de tipo exploratorio, se reveló que existen únicamente ideas vagamente relacionados con el problema de estudio para tener	Fortalezas y debilidades de los estándares aplicados			2. Las preferencias del canal de comunicación de mayor persuasión son los enlaces en sitio web y canales digitales.		2. Describir los actuales puntos fuertes y débiles en los estándares y/o protocolos de seguridad aplicados
		3. Describir los actuales puntos fuertes y débiles en	3. la segmentación de las entidades desde la perspectiva	Volumen de transacciones			Dicha investigación permitió conocer el comportamiento de compra,		3. Identificar los rubros de mayor facturación y tráfico

		los estándares o medidas de seguridad aplicadas.	adquirente se encontró con inexistencia de datos, por lo que la delimitación del tamaño de las entidades se realizó con cifras del balance se ha utilizado un cuestionario a las 60 entidades				revelando que sus consumos se orientan en supermercados, seguidamente de consumo de combustible y tiendas por departamento.		orgánico, para robustecer las medidas y/o protocolos de seguridad en sus transacciones.
		4. Evaluar el conocimiento de los usuarios activos en relación a los protocolos de seguridad incorporados en su tarjeta de crédito.		Fechas con mayor riesgo de fraude			4. El valor promedio de las transacciones realizadas por los encuestados se concentra drásticamente en un promedio mensual de L.5,000 – L.50,000. Mes: junio, julio, octubre y diciembre, por la estacionalidad e incremento en volumen transaccional. _Dia: 15-17 y 30-1 de cada mes.		4. Enumerar fechas y comercios específicos de mayor riesgo por el volumen transaccional.
				Estándares de seguridad			1. Banda magnética, 2. Chip, 3. Contactless, 4. Tokenización		

# Tarjeta de Crédito

- Versión 1 Manual de Medidas de seguridad-



<b>Documento</b>	
<b>Nombre del Documento:</b>	<b>Tarjeta de Crédito</b> <ul style="list-style-type: none"> <li>Versión 1 Manual instructivo Medidas de seguridad-</li> </ul>
<b>Ámbito de Aplicación</b>	Medios de Pago
<b>Fecha de Emisión</b>	Septiembre 2021

<b>Versión</b>	<b>Elaborado por</b>	<b>Razones de Elaboración</b>
1.0	Autor del documento	Versión Inicial <ol style="list-style-type: none"> <li>Estrategias para empoderar al usuario financiero en relación a las medidas de seguridad.</li> <li>Medidas de seguridad aplicadas por las entidades financieras que deben estar adheridas a la estrategia comercial.</li> </ol>
	Glosario	<ul style="list-style-type: none"> <li><b>Partes de una tarjeta de Crédito</b> <p><b>Banda Magnética:</b> Contiene información de la tarjeta, la misma es recibida por el terminal POS al momento de ser deslizada para compras en comercio.</p> <p><b>Chip de seguridad:</b> protección creando un código único y exclusivo para cada transacción.</p> <p><b>Número de identificación:</b> Es una serie de dígitos único.</p> <p><b>Fecha de vencimiento:</b> Posterior de esta fecha</p> </li> </ul>

		<p>se inhabilita la utilización.</p> <p><b>Nombre Cliente:</b> Cliente solicita como se describa su nombre</p> <p><b>Espacio Publicitario:</b> Destinado para el logo del ente financiero.</p> <p><b>Espacio destinado a colocar logo:</b> del emisor (marca) de la tarjeta.</p> <p><b>Espacio para la firma</b> del cliente</p> <p><b>Código CVV</b> (Código de validación) es el grupo de tres o cuatro dígitos, tradicionalmente en cursiva, sirve como medida adicional de seguridad. Conocer este código garantiza que el titular tiene físicamente la tarjeta, se utiliza en transacciones electrónicas o compras en internet</p>
--	--	---

## Manual de Medidas de seguridad- Introducción

El presente manual tiene el objetivo de definir estrategias que se deben adoptar para empoderar al usuario financiero en relación a los estándares y/o medidas de seguridad que deben considerar al realizar sus transacciones, con la debida diligencia y precaución que permita la reducción del riesgo y/o delito financiero, dichas estrategias tienen implícita la identificación en el presente manual de los canales de comunicación más efectivos y con mayor persuasión por el usuario.

Para el presente manual se consideró el creciente riesgo transaccional, por la adopción digital marcada en los últimos meses por el cambio cultural que dio apertura la pandemia COVID 19, lo que demanda la aplicación medidas y/o protocolos de seguridad más rigurosas y con mayor frecuencia, que permitan la formación del usuario y mejora continua en los estándares aplicado por el rubro financiero.

	Descripción	Ilustración
<p><b>Estrategias de Empoderamiento / Canales de comunicación</b></p>	<ul style="list-style-type: none"> <li>• <b>Cartelera Impresa</b></li> </ul> <p>Banners, Brochurs, tableros informativos y formativos, infografía.</p> <ul style="list-style-type: none"> <li>• <b>Cartelera Digital</b></li> </ul> <p>_SMS, HTML, IVR, Pagina Web, video proyectores, pantalla informativa, cartelera digital outdoor.</p> <p>_Workplace (Cliente interno)</p> <p>_Informador Oficial</p> <ul style="list-style-type: none"> <li>• <b>Enlace en sitio web</b></li> </ul> <p>Incorporar las políticas de seguridad para aceptación a través checkbox por el usuario.</p>	 <p>The illustration shows a hand holding several credit cards (red, yellow, silver) at the top. Below this are two digital banners for 'Tarjetas de Crédito'. The left banner features a man in a suit and the text 'Tarjeta de Crédito' and 'Adquiera su Tarjeta de Crédito en menos de 5 minutos'. The right banner features a woman smiling and the same text. Below the banners is a red arrow pointing right, and a red square with a white checkmark.</p>

**Estándares de Seguridad**

- **Red segura**

- \_Ejecución de transacciones seguras.
- \_PIN personal único.
- \_ATM (estación de seguridad)
- \_Canal Web (página oficial).
- \_Módulos seguros para minimizar los fraudes.

- **Protección de la información**

- \_Protección de datos de los titulares. (Incorporación de la evolución de estándares de seguridad, que salvaguarda dicha información).
- \_Redes y sistemas seguros.

- **Medida de control de acceso**

- \_Identificación única a cada usuario. (ID y/o usuario personalizado)
- \_Autorización del usuario a través de sus contraseñas.
- \_ Autenticación del usuario financiero a través de biometría.



**¿Qué es Phishing?**

Es cuando alguien se hace pasar por una identidad conocida ya sea una red social conocida, Banco, Organismo, etc. Con el fin de robarte información personal.

**¿Qué buscan robar?**

Información financiera: como números de tarjeta de crédito, número de seguridad, claves de acceso a sitios bancarios.

Nombre de usuarios de cuentas de servicio como Netflix, Facebook, etc.

Datos personales como números de teléfono, dirección de correo, etc.

**¿Cómo funciona?**

Recibes un correo que suplanta la identidad de una empresa y contiene un enlace a un sitio falso, o un archivo adjunto infectado. Si ingresas al enlace se te pedirá realizar una acción como completar un formulario con tus datos. Esa información es aprovechada para robar tu dinero o vender tus contraseñas.



\_Firma Digital del usuario.

- **Monitoreo y prueba de las redes**

\_Revisión y permiso del usuario (pantalla de autorización)

\_Procesamiento de la información con registro automático de la trazabilidad en el sistema.

\_Inclusión de herramientas de seguridad informática.

- **Políticas de seguridad de la información**

\_Segmentación de la red \_Escaneos de seguridad.

\_Controles y auditorias en el sistema para asegurar el funcionamiento de la red.

- **Puntos débiles de los estándares de seguridad**

\_Plásticos con banda magnética más expuestos a fraude mediante la utilización de Skimming (lector utilizado para el robo de información)

\_Compras en línea en sitios no



**¿Cómo protegerte?**

Presta atención la dirección remitente del correo y a la forma en que está redactado.

Desconfía de que información te solicitan.

Recuerda que ningún banco o plataforma digital te pedirá que modifiques tus datos personales a través del correo sin que tu lo hayas solicitado.

### Acciones Preventivas

- 1** Nunca te solicitarán datos por medio de correo.
- 2** No abras enlaces sospechosos
- 3** Verifica tus cuentas para evitar Phishing.
- 4** Verifica la autenticidad del sitio.

### Por tu seguridad:

Digita siempre la dirección de la página web del Banco [www.davivienda.com.hn](http://www.davivienda.com.hn)

Cuando ingreses a la banca en línea **no uses** redes públicas.

Cierra tu sesión de la banca en línea cuando termines de utilizarla.

Nunca ingreses el mismo PIN o contraseña para diferentes productos.

	<p>seguros.</p> <p>_ Comercios infringiendo protocolos de certificación del titular de la tarjeta. (Ejemplo: omiten la solicitud de identificación entre ellos, gasolineras, supermercados, restaurantes etc.</p>	
<p><b>Volumen transaccional</b></p>	<ul style="list-style-type: none"> <li>• <b>Alertas transaccionales</b> <ul style="list-style-type: none"> <li>_Notificación al usuario de consumos efectuados en su tarjeta, a través de SMS, y llamadas telefónicas por el depto. de monitoreo.</li> <li>_Alarmas generadas por incremento en transacciones. (Autorizaciones).</li> <li>_Excepción, proceso de restricción para utilización de tarjeta en el extranjero previa notificación.</li> <li>_Sistema neural para detectar los posibles fraudes</li> <li>_Inclusión de herramientas de seguridad informática.</li> </ul> </li> <li>• <b>Valores inusuales</b> <ul style="list-style-type: none"> <li>_Bloqueo preventivo mecanismo de seguridad que identifica patrones de comportamiento en sus consumos inusual.</li> </ul> </li> </ul>	 <p><b>ALERTAS POR SUS COMPRAS</b></p> <p>&gt; Realice sus compras con la mayor seguridad tanto en Honduras como en el extranjero, Habilite el servicio de alertas desde su banca por internet o llamando a nuestro Call Center. Las notificaciones le serán enviadas por mensaje de texto a su celular y correo electrónico.</p> <p><b>SEGURO CONTRA HURTO, ROBO Y EXTRAVÍO (HRE)</b></p> <p>&gt; Es un beneficio opcional que le brinda protección en sus tarjetas de crédito titular o adicionales en caso de hurto, robo o extravío a nivel nacional e internacional.</p>

	<p>_Bloqueo preventivo de facturación en comercios identificados con porcentajes significativos de fraude.</p> <ul style="list-style-type: none"> <li>• <b>Día, mes posible con riesgo de fraude.</b></li> </ul> <p>_ Mes: junio, julio, octubre y diciembre, por la estacionalidad e incremento en volumen transaccional.</p> <p>_Día: 15-17 y 30-1 de cada mes.</p>	
<p><b>Instrumentos de Investigación/Conocimiento de los usuarios</b></p>	<ul style="list-style-type: none"> <li>• <b>Conocimiento de los estándares de seguridad incorporados.</b></li> </ul> <p>_Porcentajes reducidos de usuarios que conocen los estándares de seguridad representa un 18.5%</p> <ul style="list-style-type: none"> <li>• <b>Tipo de tarjeta de Crédito</b></li> </ul> <p>_ Visa 76.2%</p> <p>_ MasterCard 15.9%</p> <p>_ American Express 7.9%</p> <ul style="list-style-type: none"> <li>• <b>Segmento de utilización de tarjeta de crédito.</b></li> </ul> <p>_ Cajeros Automáticos</p> <p>_ Pagos en línea</p> <p>_ Establecimientos comerciales.</p> <ul style="list-style-type: none"> <li>• <b>Comercios de utilización con mayor frecuencia.</b></li> </ul> <p>_ Supermercados 50.3%</p> <p>_ Gasolinera 27.8%</p> <p>_ Tienda por departamento 13.9%</p>	 <p>The image shows a smartphone screen displaying a credit card advertisement. The top part of the screen features the text 'Tarjetas de Crédito' and '¡El mundo de opciones con una sola tarjeta!'. Below this, there are several images: a hand holding a credit card, a person using a credit card at a counter, and a couple smiling. The bottom part of the screen has a red background with white text and a small image of a credit card.</p>

	<ul style="list-style-type: none"> <li>• <b>Medio digital con mayor persuasión.</b></li> </ul> <p>_Enlace sitio web 36.4%</p> <p>_Cartelera digital 31.1%</p> <p>_Cartelera impresa 7.9%</p>	
<p><b>Protocolos de seguridad para usuario/ contra fraude</b></p>	<p>_Evitar compras y/o transacciones al navegar en lugares públicos.</p> <p>_Monitoreo de transacciones periódicamente a través del portal web.</p> <p>_ Precaución al recibir correos o mensajes de texto solicitando información personal.</p> <p>_Mantener a la vista el plástico de su tarjeta, para salvar guardar el código único CVV.</p> <p>_ Cambio periódicamente de las claves y contraseñas de seguridad.</p> <p>_Evitar proporcionar información de datos sensitivos personales</p>	 <p><b>CONSEJOS PARA QUE SUS CONTRASEÑAS SEAN SEGURAS</b></p> <ol style="list-style-type: none"> <li><b>1 Usa distintas contraseñas para tus equipos y cuentas:</b> Tener la misma contraseña para ingresar a diferentes cuentas, puede traerte riesgos y permitir acceso a toda tu información.</li> <li><b>2 Utiliza combinaciones para hacer las contraseñas más seguras:</b> Si usas números, mayúsculas, minúsculas y símbolos, será más difícil que logren descifrarla. Usa mínimo ocho caracteres.</li> <li><b>3 No uses frases simples o patrones:</b> A veces recordar muchas contraseñas no es fácil, pero es muy peligroso usar palabras comunes.</li> <li><b>4 Procura no usar información personal:</b> Evita poner nombres completos, el nombre de la empresa, de tu mascota o cualquier otro dato fácil de conseguir.</li> <li><b>5 Cambia tu contraseña periódicamente:</b> Trata de cambiar tu contraseña frecuentemente. Muchos expertos recomiendan cambiarlas cada tres meses.</li> <li><b>6 Ten tus contraseñas a salvo:</b> Si se te dificulta recordar todas tus contraseñas, no las escribas todas en un solo documento, guardalas en un lugar seguro que solo tu conozcas.</li> </ol>

- **Evolución de las medidas de seguridad**

\_1Banda magnética

\_ 2Chip

\_3Contactless

\_4CVV código de verificación de 3 o 4 dígitos

\_Tokenización

\_Nombre del titular

\_Número de tarjeta de Crédito

\_Fecha de expiración

\_Firma del titular

**Medidas de seguridad implementadas**



## **REFERENCIAS BIBLIOGRÁFICAS**

- ADICAE. (2019). *Tendencias y Percepciones de los consumidores*. España.
- asociacion de los estados mericanos . (2018). *Estado de la ciberseguridad en el sector bancario en america latina y el caribe* . Canada : ciberseguridad del comite .
- Bejar, R. C. (05 de marzo de 2012).  
[https://cincodias.elpais.com/cincodias/2012/03/05/economia/1331063746\\_850215.html](https://cincodias.elpais.com/cincodias/2012/03/05/economia/1331063746_850215.html).
- Castro, J. L. (15 de 03 de 2016). <https://www.monografias.com/trabajos107/historia-banca-nacional-honduras/historia-banca-nacional-honduras.shtml>.
- Cosios, M. E. (2010).  *analisis de los medios de pago mas utilizados por los demandantes al momento de realizar sus transacciones de desembolso en la ciudad de Loja* . Loja.
- Galeano, S. (8 de Agosto de 2016). Obtenido de <https://marketing4ecommerce.net/pci-compliance-estandar-de-seguridad-ecommerce/>
- Granada, U. (s.f.). <https://www.ugr.es/~ecordon/master/docus/calculotama%C3%B1omuestra.xls>.  
Obtenido de <https://www.ugr.es/~ecordon/master/docus/calculotama%C3%B1omuestra.xls>
- IT DIGITAL SECURITY. (4 de MAYO de 2018).  *IT DIGITAL SECURITY*, 20. Obtenido de IT DIGITAL SECURITY:  
<https://www.itdigitalsecurity.es/content-marketing/2018/05/pci-dss-la-seguridad-de-los-datos-de-los-pagos-digitales-al-alcance-de-tu-mano>
- Loaiza, V. d. (2014).  *ESTUDIO EXPLORATORIO DEL USO DE TARJETA DE CRÉDITO*. LA CIUDAD DE LOJA ECUADOR: CRAI UNITEC.
- MATA, D. D. (2009).  *NUEVO ENFOQUE DEL NEGOCIO DE TARJETAS BANCARIAS EN EL SISTEMA ESPAÑOL DE MEDIOS DE PAGO*. Madrid: Tesisdoctorales.com.
- matefinanciera1. (31 de 05 de 2015). [www.monografias.com](http://www.monografias.com). Obtenido de <https://matefinancieraumg.wordpress.com/2015/05/31/historia-de-las-tarjetas-de-credito/>.
- non-commercial(BY-NC), A. (20 de 05 de 2013).  *Variables e Indicadores*. Obtenido de <https://www.scribd.com/doc/142647647/las-variables-e-indicadores-en-la-ivestigación>
- NVINDI. (21 de Junio de 2019). Obtenido de <https://www.mejorestarjetasdecredito.es/que-son-las-tarjetas-emv/>
- OLAVARRIETA, G. E. (2012).  *METODOLOGIA PARA MEDIR LOS EFECTOS DE LA APLICACION DE ESTANDARES SOBRE LA INDUSTRIA DE LOS MEDIOS DE PAGO EN EL MERCADO CHILENO*. CHILE.
- Vieda, M. (01 de Diciembre de 2010).  *Estandar de seguridad de datos para la industria de pagos con tarjeta*. Obtenido de Software Engineer: <https://maelvieda.com/blog/estandar-de-seguridad-de-datos-para-la-industria-de-pagos-con-tarjeta/>

## ANEXOS

### SU SEGURIDAD ES IMPORTANTE AL UTILIZAR SUS TARJETAS DE CREDITO COMO MEDIO DE PAGO

Soy estudiante de la facultad de postgrado de UNITEC, pasantes de la Maestría en Dirección Empresarial, y estoy realizando un estudio sobre la Evolución de las tarjetas de crédito como medio de pago seguro.

Solicito su valioso tiempo, para llenar la siguiente encuesta con el objetivo de evaluar su conocimiento en relación a los estándares de seguridad incorporados en su Tarjeta de Crédito.

**INSTRUCCIÓN:** Marque con una “X” la respuesta a la interrogante según sea su criterio y conocimiento.

#### **I. Datos generales**

1. Género M\_\_\_ F \_\_\_
2. Edad \_\_\_
3. Actividad que realiza \_\_\_\_\_
4. Estado civil \_\_\_\_\_

#### **II. Información financiera**

Seleccione una de la opción de respuesta a la interrogante conforme su conocimiento.

1. ¿Cuenta usted con tarjeta de crédito? ¿Cuántas?
  - a. 1
  - b. 2
  - c. 3
  - d. 4 o más
  
2. Si su respuesta es afirmativa que tipo de tarjeta posee?
  - a. Visa
  - b. MasterCard
  - c. Discover
  - d. American Express
  - e. Todas las anteriores
  
3. ¿Hace cuánto tiempo posee tarjeta de crédito?
  - a. 1 – 10 años
  - b. 10 - 15
  - c. 15 - 20
  - d. 20 o más

4. ¿En qué comercios utiliza con mayor frecuencia su tarjeta de crédito como medio de pago? Marcar la que más.

- Tiendas por departamento
- Gasolinera
- Supermercado
- Ferretería
- Farmacia
- Escuelas, colegio, Universidades

5. ¿Cuál es el valor promedio que cancela a través de su tarjeta de crédito mensualmente?

- a. 10,000 -100,000
- b. 100,001- 200,000
- c. 200,001-300,000
- d. 300,001- o más

6. ¿Conoce los estándares de seguridad de su tarjeta de crédito contra fraude?

- a. si
- b. no

7. ¿Cuál de los siguientes estándares de seguridad usted conoce?

- a. Banda Magnética
- b. Chip
- C. Contactless
- d. Todas las anteriores
- e. Ninguno de los anteriores

8. Sabe para qué sirve la Banda Magnética?

- a. si
- b. no

9. Para qué sirve el Chip en una Tarjeta de Crédito?

- a. si
- b. no

10. Para qué sirve el pago sin contacto (Contactless) en una Tarjeta de Crédito?

- a. si
- b. no

11. Si su respuesta fue afirmativa ¿Porque tipo de medio digital los conoció?

- a. Cartelera Impresa
- B. Cartelera Digital
- C. Enlace Sitio WEB

12. Considera que las tarjetas de crédito como medio de pago es segura para realizar sus

transacciones?

- a. si
- b. no

13. Realiza revisión continua en la página web de los consumos realizados?

- a. si
- b. no

14. Realiza cambio periódicamente de sus contraseñas y claves en la plataforma virtual?

- a. si
- b. no

15. Como medida de seguridad registra su firma en la tarjeta de crédito?

- a. si
- b. no

16. ¿Para qué sirve el CVV de verificación de 3 dígitos incorporados en su tarjeta de crédito?

¡Muchas gracias por su tiempo!

## ENTREVISTA

**Nombre del Entrevistado: Ingeniero Fabio Tabora**

**Ocupación: Director de Tarjera de Crédito**

**Empresa: Banco Davivienda S.A.**

1) ¿Cuál ha sido la evolución de tarjetas de crédito como medio de pago?

R/ \_\_\_\_\_  
\_\_\_\_\_

2) ¿Cuáles son los pasos de la evolución de tarjetas de crédito?

R/ \_\_\_\_\_  
\_\_\_\_\_

3) ¿En relación a la vulnerabilidad de las transacciones impacta al ente financiero o usuario?

R/ \_\_\_\_\_  
\_\_\_\_\_

4) ¿Considera que los estándares de seguridad actuales tienen una cobertura óptima?

R/ \_\_\_\_\_  
\_\_\_\_\_

5) ¿Considera que, si se empodera el conocimiento de los usuarios en relación a los estándares de las tarjetas de crédito, mitigaría el riesgo para las entidades financieras?

R/ \_\_\_\_\_  
\_\_\_\_\_

6) ¿Cuál es el medio más óptimo para comunicar a los clientes?

R/ \_\_\_\_\_  
\_\_\_\_\_

¡Muchas gracias por su tiempo!

## **Glosario**

**Contactless:** es el término que se aplica a la tecnología que permite realizar operaciones ‘sin contacto’ mediante un sistema de comunicación denominado NFC (‘near field communications’). Se utiliza principalmente con tarjetas de crédito, pero cada vez hay más dispositivos plásticos que admiten esta tecnología, como teléfonos móviles, relojes inteligentes o llaveros.

**Código CVV** (Código de validación) es el grupo de tres o cuatro dígitos, tradicionalmente en cursiva, sirve como medida adicional de seguridad. Conocer este código garantiza que el titular tiene físicamente la tarjeta, se utiliza en transacciones electrónicas o compras en internet

**Banda Magnética:** Contiene información de la tarjeta, la misma es recibida por el terminal POS al momento de ser deslizada para compras en comercio.

**Chip de seguridad sistema EMV:** protección creando un código único y exclusivo para cada transacción.

**Número de identificación:** Es una serie de dígitos único.

**La tokenización:** es el proceso que permite proteger datos sensibles, sustituyéndolos por equivalentes no-sensibles, conocidos como tokens. Un token en sí no tiene ningún valor o significado, es una referencia o identificador que, gracias al sistema de tokenización, permite volver al dato sensible. La tokenización se utiliza para evitar el robo de datos en las transacciones con tarjetas bancarias.

**Fecha de vencimiento:** Posterior de esta fecha se inhabilita la utilización.

**Estándares de seguridad:** tienen como objetivo unificar las medidas de seguridad de las tarjetas de crédito en todo el mundo. El PCI DSS fue redactado originalmente por un grupo

conocido como PCI Security Standards Council.

**IVR:** es una tecnología de telefonía automatizada que interactúa con las personas que llaman, recaba la información requerida y enruta las llamadas al destinatario o bien al sector apropiado dentro de la empresa.