UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de Información

AUTOR:

Montalvo Vivar, Carlos Javier (ORCID: 0000-0002-2746-2630)

ASESOR:

Dr. Martínez López, Edwin Alberto (ORCID: 0000-0002-1769-1181)

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones

Lima – Perú

2022

DEDICATORIA

Mi tesis la dedico a mi esposa Marisol quien desde hace 7 años atrás me impulso a seguir esta aventura académica en la universidad para cumplir mi sueño de ser docente y dar oportunidad a otros en seguir aprendiendo.

AGRADECIMIENTO

Agradezco a mi familia en acompañarme a esta aventura que empezó hace 7 años y por supuesto a la universidad en haber contribuido en mi formación profesional.

Índice de contenidos

Índices de tablas

Índices de gráficos y figuras

RESUMEN

La presente investigación tuvo como objetivo general proponer la implementación de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras. El enfoque de la investigación fue cualitativo, el método de la investigación se basó en el paradigma interpretativo, el tipo de investigación fue básica y se usó el diseño investigación acción. Se utilizó como técnicas de investigación la entrevista semiestructura, la observación y por último el análisis documental. La técnica de triangulación se utilizó para dar respuesta a los objetivos y conclusión.

Se concluye que para la protección de los datos de las tarjetas de pagos se requiere implementar estándares de seguridad que estén orientados en asegurar los tres pilares de seguridad como la disponibilidad, la confiabilidad y la integridad de la información, sin embargo estos estándares deben de ir acompañados de mecanismos que permitan gestionar la seguridad en el almacenamiento, en el procesamiento y trasmisión de los datos, además deben de estar alineados con la infraestructura implementada. Por otra parte, la mejor manera de reducir el fraude cibernético, en ATM, canales electrónicos y punto de venta es con la implementación de sistemas biométricos y de herramientas de autoaprendizajes.

Palabras clave: Inteligencia artificial, Pilares de seguridad, Patrones de comportamiento

ABSTRACT

The general objective of this research was to propose the implementation of security standards for the protection of payment card data in financial institutions. The research approach was qualitative, the research method was based on the interpretive paradigm, the type of research was basic, and the action research design was used. The semi-structural interview, observation and finally documentary analysis were used as research techniques. The triangulation technique was used to respond to the objectives and conclusion.

It is concluded that for the protection of payment card data it is necessary to implement security standards that are oriented towards ensuring the three pillars of security such as availability, reliability and integrity of the information, however these standards must go accompanied by mechanisms that allow managing security in the storage, processing and transmission of data, in addition they must be aligned with the implemented infrastructure. On the other hand, the best way to reduce cyber fraud, in ATM, electronic channels and point of sale is with the implementation of biometric systems and self-learning tools.

Keywords: Artificial intelligence, Security pillars, Behavior patterns

I. INTRODUCCIÓN

Es importante que las entidades financieras implementen o creen mecanismos de seguridad apropiados para garantizar el acceso oportuno a los datos de las tarjetas de pago, es por eso la importancia de la implementación de estándares de seguridad para reducir el riesgo de un acceso no autorizado en aquellos dispositivos electrónicos que procesan, transmiten y almacenan datos confidenciales de los tarjetas habientes y que se utilizan como medio para realizar transacciones financieras desde los distintos canales virtuales. Asbanc (2021) sostuvo que, hoy en día el canal virtual más utilizado en el Perú es la Banca móvil, es decir ha pasado del 8.3% de transacciones realizadas al 46.1% después de la pandemia y de incidentes reportados del 27.3% al 70.8% a nivel nacional. Por otro lado, el BCRP (2020), afirma que, se ha incrementado el uso de pagos de productos y servicios por celular del 1% al 26% entre el 2013 y el 2019.

Las entidades financieras son las que han incentivado el uso de las tarjetas de pago con el propósito de que los clientes utilicen con mayor frecuencia el dinero electrónico sin dejar de lado la seguridad de los datos de los tarjetas habientes. Al respecto, Balagolla et al. (2021) sostuvo que con la rápida expansión de las transacciones, el término de la tarjeta de crédito se hizo muy conocido, lo cual motivo que su uso sea masivo, en esta interacción trabajan los mismos clientes, comerciantes y los operadores de tarjetas, la globalización tecnológica ha impulsado el uso de tecnologías emergentes como la Blockchain para la gestión de tarjetas de pago, bancos como JP Morgan, HSBC, BBVA, Santander y el BCP ya están en el proceso de usar Blockchain para el intercambio de transacciones financieras.

Por otro lado, la tecnología cumple un papel fundamental a nivel de seguridad para generar confianza entre los clientes, al respecto, Ayo C.K et al. (2021) afirmó que Nigeria adopto una política de reducción de efectivo a través de una sistema de verificación biométrico, esta política impulso a las TIC a trabajar de manera más eficiente en el uso de las tarjetas de pago con la finalidad reducir fraudes y corrupción en la sociedad y fomentar el uso del dinero electrónico. Asimismo, Bielefeld S et al. (2021) afirmó que el concepto del uso de la tarjeta de débito sin efectivo es más complejo de fomentar en los países occidentales.

Hoy en día, las entidades financieras en Perú han implementado a lo largo del tiempo mecanismos de seguridad a nivel de software y de hardware para reducir el acceso no autorizado de las tarjetas de pago. Al respecto, King S.T et al. (2021) sostuvo que los fraudes por el uso de tarjetas de pago se estiman en una pérdida de 130 millones de dólares entre el 2018 y 2023 a nivel mundial además que para prevenir esta situación se requiere de soluciones explícitamente técnicas. Asimismo Yadav A et al. (2020) indicó que una forma de reducir el fraude en las tarjetas de pago es con la implementación de algoritmos de autoaprendizaje para realizar predicciones. Asimismo, la revista información (2019) resaltó que el 90% de entidades financieras en América del norte, Europa y Asía utilizan usan Machine Learning. El peruano (2021), afirmó que en el sector financiero peruano su adopción aún está siendo evaluada.

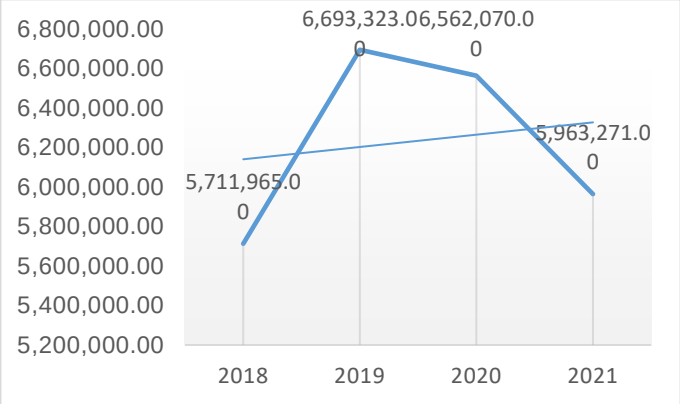
Si bien es cierto, las entidades financieras a lo largo del tiempo se han preocupado en implementar soluciones informáticas para brindar una seguridad adecuada, la protección de los datos de las tarjetas de pago se ha convertido en un elemento importante ya que sin los mecanismos adecuados para controlar la transmisión, el proceso y el almacenamiento a los datos de los diferentes equipos informáticos se puede comprometer al fraude y la divulgación de los datos confidenciales. El uso inadecuado por parte de personas inapropiadas puede generar diferentes sanciones, como multas, y una mala imagen reputacional a la entidad financiera lo cual significaría una reducción en la confianza comercial de los clientes y en la contratación de los servicios bancarios. Al respecto, Í. Erdoğan et al. (2020) sostuvo que para la detección de fraudes en los sistemas de comercio electrónico se viene utilizando inteligencia artificial y aprendizaje automático.

Por otra parte, en Perú de acuerdo a la SBS (2019) indicó que, se debe de cumplir con todos los requerimientos de seguridad que indica la norma PCI-DSS para todas las entidades financieras, el cual indica la implementación de una red segura, evitar la parametrización de configuraciones por defecto, cifrado de los datos, truncamiento de información en los sistemas informáticos, mantener una política de instalación de antivirus, parches de seguridad, contar con lineamientos para el control de acceso, autenticación, conservar eventos de auditoria y finalmente contar con capacitaciones oportunas a los colaboradores para el manejo de los sistemas tecnológicos. En las figuras se muestra dicho comportamiento.

En Perú, entre el 2018 y 2021 se cuenta con más de 6M de tarjetas de crédito visa emitidas entre entidades bancarias y financieras y de acuerdo a los datos estadísticos, la tendencia de la emisión de las tarjetas de crédito fue a la baja debido principalmente a que el índice de morosidad tuvo un incremento del 2% por endeudamiento financiero entre julio 2020 y mayo 2021, tal como se indica en figura 1 y 2.

Figura 1

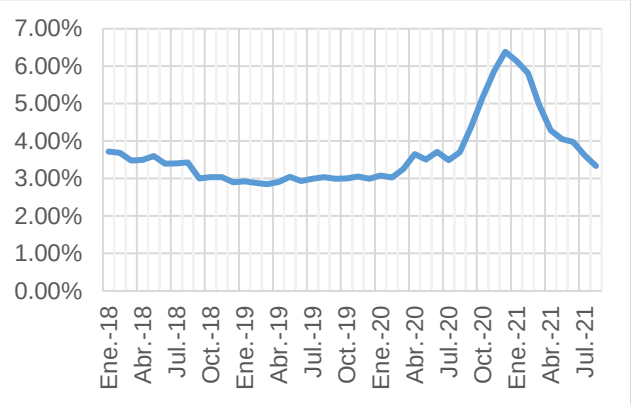
Emisión de tarjetas de crédito 2018 – 2021



Fuente: ASBANC

Figura 2

Morosidad de clientes



Fuente: ASBANC

De acuerdo a esta realidad problemática, la presente investigación tiene como enunciado del problema general lo siguiente ¿Cuál es la situación actual de los estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021? Y como enunciado de problemas específicos (a) ¿Cómo es la disponibilidad de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?, (b) ¿Cómo es la confidencialidad de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?, (c) ¿Cómo es la integridad de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?, (d) ¿Cómo es el acuerdo de servicio de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?

Respecto a la formulación del objetivo general se plantea lo siguiente Proponer la implementación de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021 y como enunciado de los objetivos específicos (a) Determinar la disponibilidad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021, (b) Determinar la confidencialidad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021, (c) Determinar la integridad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021 (d) Determinar los acuerdos de nivel de servicio en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021.

Por otro lado, se tiene una justificación tecnológica el cual manifiesta que implementando un estándar de seguridad permitirá a las entidades financieras reducir el riesgo de personas o procesos no autorizados tengan acceso a datos confidenciales de las tarjetas de pago a través de mecanismos informáticos que permitan monitorear alertas y configuraciones sospechosas. Asimismo, se tiene una justificación económica que sostiene que implementando un estándar de seguridad permitirá reducir pérdidas monetarias, sanciones regulatorias, una mala imagen institucional tanto a los clientes como a los entes supervisores en caso de algún incidente de fraude cibernético, por otro lado se presenta una justificación práctica, aquí se propone implementar una solución tecnológica que permita mantener la disponibilidad, confiabilidad, integridad y un acuerdo de nivel de servicio en los dispositivos electrónicos que procesen, transmiten y almacenen datos de tarjetas de pago dentro de la red de la entidad financiera con la finalidad de aumentar la confianza de los consumidores y por consiguiente el uso de los servicios y productos para generar más ingresos y fidelización. Ver anexo 9.

II. MARCO TEÓRICO

A continuación, Albornoz et al. (2017) indicó que, de acuerdo a una encuesta realizada en Perú, el 75% de los encuestados no usa el aplicativo móvil debido a la falta de seguridad al realizar las transacciones financieras por motivos de fraudes cibernéticos sin embargo para remediar este tipo de incidentes el autor sugirió la aplicación del estándar de seguridad PCI-DSS con la finalidad de mejorar la gestión, configuración, procedimientos y arquitectura tecnológica. Asimismo, Meléndez (2020) sostuvo que, con la utilización de una herramienta centralizada en donde se concentre la mayor cantidad de entidades financieras y se utilice para realizar operaciones bancarias permitirá prevenir, detectar y reducir el riesgo de fraude electrónico de los clientes a través de mecanismos seguros peer to peer.

A propósito, Farfán (2015), indicó que, del 99.26% del empresariado nacional (micro, pequeñas y medianas empresa) solo el 23% acepta pagos electrónicos con tarjetas de crédito o débito, lo cual hace notar una brecha importante debido a los altos costos de comisiones, esto empuja a contar con una aplicación móvil que permita ser una pasarela de pago pero con mecanismos de seguridad, como el antivirus para la eliminación de virus maliciosos en el sistema operativo, test de penetración para simular un ataque, OSSTMM (Open Source Security Testing Methodology) análisis de seguridad y el OWASP que sirve para verificar código inseguro. Por otra parte, El BCRP (2015), sostuvo que, las medidas de seguridad implementadas en el mercado financiero para reducir fraudes son, uso de tarjetas con chip; envío de mensajes de alerta; Bloqueo automático; Seguro por fraude; Difusión sobre medidas de seguridad y entrenamiento en los comercios.

Por su parte, Calderón (2019) indicó que, el uso de internet, el mejoramiento en los protocolos de seguridad y el uso masivo de los teléfonos inteligentes han hecho que los medios de pagos más usados sean los pagos con tarjeta y transferencias bancarias en LATAM, en el 2011 las transferencias alcanzaron el 74% y en el 2016 alcanzaron el 84% del valor de las operaciones, dentro de los principales retos a superar siguen siendo a) asegurar que las personas no autorizadas accedan a información confidencial; b) autenticar el receptor de la información y finalmente comprobación de firmas digitales

En igual forma, Chaithanya et al. (2021) quien concluyó que, para reducir el fraude en las transacciones financieras es necesario la implementación de dispositivos biométricos como la huella digital además que esta tecnología permitirá evitar el transporte de la tarjeta en físico. Asimismo, Benamara et al. (2021) sostuvo que, para reducir las vulnerabilidades en el acceso a los datos de un cliente a través de los terminales de pago es importante combinar la tecnología RFID (Identificación de radio frecuencia) con inteligencia artificial mediante un sistema biométrico facial. También, El Madhoun.et al. (2020) precisó que, la comunicación entre el punto de venta y la tarjeta de pago del cliente debe de estar asegurada mediante mecanismos de encriptación como el protocolo EMV ya que la transacción almacena datos sensibles.

Otro resultado fue el de Spring et al. (2021) quien afirmó que, si bien es cierto y a pesar que el CVSS se utiliza para analizar las vulnerabilidades de los softwares no se debe de utilizar para gestionar los riesgos además los autores precisan que es importante determinar proveedores de escaneo aprobados para dicho fin. Asimismo, Bestami et al. (2020) concluyó que, los algoritmos de aprendizajes son herramientas que se utilizan para detectar los fraudes con las tarjetas de pago a través de diferentes métodos, por ejemplo KNN (K-Nearest Neighbor Method) el cual usa como condición valores atípicos de un conjunto de datos.

Además, Bojjagani et al. (2021) sostuvo que, los equipos móviles son en la actualidad los dispositivos más utilizados para realizar transacciones financieras, como consultas, pagos y compras ONLINE a comparación de otros canales electrónicos como el ATM o la banca por internet, con el fin de que las transacciones sean más seguras, se sugiere aplicar tres mecanismos de seguridad como son la seguridad a nivel de aplicación, comunicación y de dispositivo. Asimismo, Sitek et al. (2020) sostuvo que, para incrementar la seguridad de las transacciones financieras en los diferentes canales electrónicos en vez de solo utilizar el PIN se podría utilizar un mecanismo de reputación o perfil como por ejemplo hábitos de compra, frecuencia y volumen para la protección de los sistemas de pagos.

También, Boureanu et al. (2020) quien concluyó que, para reducir el acceso no autorizado a las tarjetas de pago es requerido que el protocolo de seguridad EMV (Europay Mastercard Visa) este constantemente actualizado. Asimismo, Nasution, et al (2020), sostuvo que, la tecnología de reconocimiento facial tiene más beneficios de seguridad que el uso del PIN (Pesonal Identification Number), una de las ventajas es evitar el fraude de identidad, robo del PIN y uso de la tarjeta de pago. También, Busse et al. (2020) sostuvo que, los métodos de pagos depende en gran medida de las culturas de los países, por ejemplo en China e Irán tienen mayor preferencia al uso del PIN para realizar transacciones financieras que a diferencia de Alemania y USA que están utilizando el uso de pagos por criptomonedas.

De la misma forma, Nyarko-Boateng et al. (2020) sostuvo que, para reducir el fraude y mejorar la seguridad en las transacciones de pago electrónico en línea es necesario optimizar el proceso de autenticación de los datos entre el dueño de la tarjeta y el banco a través de mecanismos de control del CVV (Card Verification Value). Asimismo, Karrupusamy et al. (2020) concluyó que, el algoritmo C18 proporciona una mejor precisión de resultados para la detección de fraude con las tarjetas de crédito, esto permitirá evitar que personas no autorizadas tengan acceso a las transacciones. También, Samaranayake et al. (2019) afirmó, que para garantizar la confidencialidad y disponibilidad de la información de las tarjetas de pago desde un POS (Point of sale) es importante implementar mecanismos como malware para detectar y prevenir ataques, BOT para prevenir y verificar el estatus del sistema y además DLP (Data leakage Prevention) para prevenir fuga de datos.

Por otro lado, Rahaman et al. (2019) Indicó que, que la implementación del estándar de seguridad PCI DSS permite reducir las vulnerabilidades de seguridad sin embargo existe una gran brecha entre las especificaciones y su aplicación, 60 millones de tarjetas de pago se vieron comprometidas en el 2018 y en el 2013 se filtró información de los datos de las tarjetas de pago de aproximadamente de 40 millones en los estados unidos. Asimismo, Feofilova et al. (2019) sostuvo que, existen amenazas tecnológicas que comprometen la seguridad nacional de la federación de Rusia a través de medios digitales y que se derivan por la falta de obtener datos estadísticos de las transacciones financieras.

Al mismo tiempo, Ajay Chowdary et al. (2019) concluyó que, para reducir los incidentes de fraudes a nivel mundial que entre el 2003 y el 2014 ha llegado del 0.2 M a 1.6 M es requerido implementar soluciones sofisticadas que compliquen al atacante tomar control de las tarjetas de pago, en este caso el autor propone que a través de un sistema de geolocalización la transacción sea efectiva cuando la ubicación de la tarjeta y del móvil sea la misma. Asimismo, Larisa et al. (2019) sostuvo que, la tendencia en el sistema financiero son los bancos digitales llamado neobancos, Al cierre del 2016 el Reino Unido tiene el mayor número de neobancos (40) seguido de la India (8), Estados Unidos (5), Francia (4), Alemania (3) y China (3). Por otro lado, Kaur et al. (2018), indicó que, los fraudes por el servicio de ATM va en aumento, al menos el 14% de fraudes han sido por clonación de tarjetas de pago en ATM el cual han ocasionado pérdidas de mil millones de dólares en la India y se sugiere reformular las leyes para reducir estos tipos de crímenes.

Por otro lado, Saxena et al. (2019) sostuvo que, en la India entre Marzo 2016 y Marzo 2017 se han realizado alrededor de 342 billones de transacciones en línea, esto ha demandado evaluar diferentes métodos de seguridad y uno de ellos es el marco de seguridad llamado CIA (Confiabilidad, Integridad y Disponibilidad), el cual está enfocado en mejorar el proceso de autenticación, autorización, confidencialidad, integridad, no repudio, hostilidad y seguridad de la información. También, Saia et al. (2018) sostuvo que, la tecnología de Big Data asume un papel fundamental para la detección de fraudes debido principalmente a dos factores, el primero al crecimiento exponencial del comercio electrónico y el segundo al crecimiento en el uso de las tarjetas de pago.

En adelante, Bataev et al. (2019) concluyó que, existe una corriente a nivel mundial de realizar las transacciones sin efectivo, alrededor del 30% de las operaciones son con tarjeta de pago y que de acuerdo a las estadísticas el país que menos efectivo usa es Singapur con un 71% de operaciones, más del 70% de operaciones en el mundo son aún en efectivo es por ese motivo que la seguridad en los ATM se inclina en la implementación de reconocimiento facial. Asimismo, Alemu et al. (2015) sostuvo que, en los países de bajos ingresos como por ejemplo en el caso de Ethiopian se utiliza en gran medida los ATM debido a la influencia social y la credibilidad percibida de estos servicios, aún existe una baja inversión en soluciones tecnológicas.

A continuación, las categorías y sub categorías que he propuesto son las siguientes, La disponibilidad, es un principio de la seguridad que permite tener acceso permanente a los recursos informáticos para la continuidad de los servicios con la finalidad de responder oportunamente las transacciones financieras, la disponibilidad trabaja de la mano con la implementación de las buenas prácticas tecnológicas como por ejemplo la activación de un DRP (Disaster Recovery Planning), la configuración de alta disponibilidad en modo CLUSTER, la adopción de estándares de seguridad como ISO 27001 o PCI DSS y estándares de arquitectura como ITIL. An et al. (2021) sostuvo que, debido a los constantes ataques de denegación de servicio (DoS) en los enlaces de Internet se recomienda la implementación de la tecnología MMP (Multi-Hop Multi Path) es decir que exista varias rutas de acceso con la finalidad de evitar la indisponibilidad de los servicios.

En relación a, la sub categoría configuración de firewall es un elemento fundamental que permite restringir el direccionamiento interno y externo entre las diferentes redes de la organización. Sahi et al. (2017) concluyó que, los servicios en la nueva era han aumentado de manera exponencial por tal motivo la implementación de un sistema de detección y prevención son requeridos, el primero permite identificar los mensajes maliciosos y el segundo permite denegar el acceso, por lo general los ataques de DoS (Denial of Service) inundan de paquetes a los equipos de seguridad y saturan el ancho de banda, el beneficio de contar con equipos de seguridad es controlar la interconexión entre redes públicas y privadas a través de políticas específicas en donde se configure direccionamiento origen, puertos seguros, NAT (Network Address Translation) y direccionamiento destino.

Asimismo, las contraseñas que no son robustas permiten que personas no autorizadas tengan acceso a la organización. Chowdhury et al. (2020) indicó que, si bien es cierto en Bangladesh enfrentan continuas amenazas cibernéticas, el fraude sigue siendo uno de los factores principales de pérdidas financieras de servicios en línea, es por ese motivo que para reducir el acceso no autorizado en Bangladesh, se implementó 6 tipos de contraseñas heurísticas, como ejemplo, guías para la construcción de las contraseñas, mecanismo para la recuperación de contraseñas, utilización de CATCHA, preguntas de seguridad, utilización de HTTPS y medidor de contraseña, de acuerdo al informe, hasta el 2020 se han utilizado alrededor de 300,000 millones de contraseña.

La confidencialidad hoy en día se ha convertido en un lujo debido a que para lograrlo hay que implementar equipos de tecnología altamente sofisticados y que además se debe de contar con grandes presupuestos sin contar que el equipo humano debe de estar calificado para estar atento a los indicios, por otro lado, un elemento significativo es la proceso de monitoreo el cual permitirá reaccionar con el tiempo suficiente ante un ataque y sobre todo tomar acción de acuerdo al protocolo estipulado. Georgieva et al. (2019) sostuvo que, Las aplicaciones de redes neuronales sirve para detectar y prevenir los fraudes, el objetivo de la detección de fraudes con tarjetas de crédito es decidir si una transacción es fraudulenta basándose en patrones de datos históricos de acuerdo a atributos como el destinatario, monto y fecha de la transacción, es por ello que se debe de implementar mecanismos de seguridad para el mal uso de los datos.

Por otro lado, la protección del almacenamiento de los datos es proceso sensible debido al contenido y al uso que se le pueda dar en caso que personas no autorizadas tengan acceso, los controles se deben de enfocar por segmentar un perímetro de seguridad, mantener una política de respaldo y actualizar con alguna frecuencia parches de seguridad y sistema operativo. Georgieva et al. (2020) concluyó que para proteger los datos confidenciales almacenados en servidores físicos o virtuales de las entidades financieras es importante seguir el estándar PCI. En suma, es importante determinar un inventario de activos de la información para implementar políticas y herramientas que permitan el control del acceso.

Por otra parte, el cifrado de los datos está orientada tanto a nivel de aplicación como redes para evitar la materialización de los ataques como hombre en el medio o de diccionario. Asimismo Daud et al. (2018) concluyó, el cifrado de datos permite asegurar la confidencialidad de la información de punto a punto a través de protocolos como AES, 3DES o DES sin embargo el cifrado de la información genera un mayor rendimiento de latencia, paquetes perdidos y velocidad y que el cifrado AES es el que tarda mucho más para transferir archivos por la red. El cifrado de datos permite evitar que se comprometa los datos sensibles de las tarjetas de pago sin embargo esta arquitectura debe ser implementada en cada punto remoto de la organización además se debe de tomar en cuenta las capacidades tecnológicas de los equipos de comunicación para que no generen saturación en memoria o procesador.

Adicionalmente, la sub categoría restringir el acceso físico a los datacenter, este lineamiento permite controlar la entrada y salida de las personas y a través de una bitácora se llevará el control de las actividades a realizar. Dumsky et al. (2015) afirmó que, los centros de datos han sido diseñados para albergar equipos, almacenar datos, procesar información y dar seguridad con la finalidad de proporcionar calidad, existen 4 categorías, TIER 1, la disponibilidad es 99.67% con 28 horas de interrupción, TIER 2, con 99.75% y 22 horas, TIER 3, con 99.98% y 1.6 horas N+1, finalmente TIER 4, con 9.99% y 0.8 horas respectivamente.

Continuando, la categoría de integridad, este un elemento fundamental para asegurar que el dato permanezca intacto a lo largo de su ciclo de vida, para que la integridad de los datos se mantenga, es necesario que no haya habido cambios o alteraciones en los datos ya sea en la transmisión, en el proceso o en el almacenamiento es por eso la importancia de aplicar mecanismos de seguridad que aseguren o controlen los accesos no autorizados. Yeh et al. (2020) sostuvo que, la operadora de tarjetas de pago visa utiliza un modelo llamado multimodal que no es más que un método de auto aprendiza para detectar los fraudes, la técnica es no solo generar patrones individuales por tienda comercial o por consumidor sino más bien por afinidad o correlacional para mejor el nivel de acierto, la identificación comerciante-consumidor es importante para garantizar la integridad del procesamiento de pagos.

Dentro de las subcategorías tenemos el antivirus, este mecanismo de defensa heurístico ha cobrado más protagonismo conforme creció la demanda de ataques a los distintos dispositivos electrónicos, desde una máquina de escritorio hasta un equipo móvil, hay que tener en cuenta que los nuevos desarrollos de virus no solo modifican los datos sino también reducen su acceso a través del cifrado de la información lo cual hace más difícil la operatividad de los negocios. Li et al. (2019) concluyó que, si bien es cierto los ataques a las vulnerabilidades de la micro arquitectura son catastróficas, se puede detectar a través de las desviaciones de comportamiento de los contadores del proceso de rendimiento, los ataques tipo RowHammer explotan la vulnerabilidad de la DRAM. La adopción de políticas de seguridad de antivirus permitirá identificar los dispositivos electrónicos riesgosos y aplicar el software antivirus más adecuado para la protección de ataques.

Ahora bien, la sub categoría protocolos seguros nos indica que para reducir la manipulación de los datos en caso de un ataque, como por ejemplo de DoS (Denied of Service), hombre en el medio o de virus es importante utilizar protocolos que permitan proteger los datos como es el caso del HTTPS, SFTP, SSH entre otros. Thomas et al (2020) finalmente mencionó, que para detectar ataques de inyección, configuración incorrecta, se requiere de una herramienta capaz de analizar la cabecera (URL) y el cuerpo de la página WEB para que luego del análisis, este pueda enviar un alerta. De igual modo, para reducir la alteración de los datos se sugiere utilizar el protocolo HTTPS para el acceso a páginas WEB.

Además, la asignación de acceso a los componentes del sistema nos indica que los usuarios deben de contar solo con los accesos requeridos de acuerdo a su función para la actualización de los datos en el sistema, esta modificación debe de estar aprobada y controlada a través de un requerimiento o por un incidente mediante herramientas informática. Del mismo modo Arora et al. (2021) sostuvo que el acceso no autorizado a los datos en un DW (Data warehouse) puede provocar corrupción de datos, robo de información y denegación del servicio, en ese sentido el autor propone la implementación de un IDS (Intrution Detection System) con segundo nivel de autenticación para alertar al administración en caso de patrones de ataque o de desviación de comportamientos de usuarios, esta técnica permitió una reducción del 18% de los falsos negativos y una reducción del 64% de los falsos positivos. Los niveles de acceso deben ser homologados y específicos para reducir la gestión de alertas.

Por otra parte para cumplir con los acuerdos de nivel de servicio es necesario identificar los dispositivos electrónicos, determinar los indicadores de rendimiento y monitorearlos a través de un tablero de control. De La misma manera Zhao et al. (2021) concluyó que, la implementación del FRAN (Fog Radio Access Network) permite reducir la congestión y latencia de los servicios por la red a través de nodos distribuidos con una arquitectura segmentada, esto permite que los usuarios accedan a sus aplicaciones de manera más oportuna, esta técnica está acompañada del SSLA (Secure-Service level agreement) el cual permite asegurar cada nodo y enlace físico para defender de ataques. Para terminar, los SLA permiten monitorizar todos los dispositivos de la red para asegurar el correcto funcionamiento a nivel de arquitectura y de seguridad.

El mantenimiento preventivo, se refiere al proceso de validar el correcto funcionamiento de los dispositivos tecnológicos tanto físico como lógico. Ahora bien Larbi Rebaiaia et al. (2020) nos comentó que, que el principal objetivo de una política de mantenimiento es realizar acciones de mantenimiento al menor costo a través de tres estrategias; a) reparaciones mínimas en caso de fallas b) reemplazo completo en la primera falla y por último c) reemplazo completo en cada falla siendo esta la más eficiente en la reducción de costos. De esta manera, es importante formular un cronograma de planificación de mantenimientos para reducir los costos operativos a nivel de negocio con la finalidad de que los equipos tecnológicos estén disponibles los 365 días del año.

Asimismo, el mantenimiento correctivo, es un proceso que tiene como objetivo el reemplazo de partes y piezas de un dispositivo tecnológico con la finalidad de reestablecer los servicios involucrados. Por otra parte Lai et al. (2019) concluyó que los mantenimientos correctivos tradicionales están siendo reemplazados por los CBM (Condition base maintenance) a través del IoT con la finalidad de mejorar la seguridad y confiabilidad de los equipos tecnológicos es decir prolongando su vida útil, reduciendo incidentes e interrupciones al negocio de una manera más predictiva mediante la recopilación, análisis de los datos y la toma de decisiones. En suma, es importante contar con un contrato de soporte que permita suplir las partes y piezas comprometidas para reducir el RTO (Recovery time objetive) e impactar en menor tiempo al negocio.

Igualmente, el impacto de análisis de negocio permite determinar las aplicaciones críticas de la organización para planificar la seguridad y arquitectura más adecuada con la finalidad de acceder de forma oportuna a los servicios en caso de la ocurrencia de algún incidente y desastre. Agregando a lo anterior, Radkov et al. (2018), sostuvo que, la clasificación de aplicaciones críticas de acuerdo a la arquitectura tecnológica es obsoleta y que más bien debería ser mediante indicadores tales como operaciones de la organización y amenazas actuales, la finalidad del BIA (Business impact analysis) es evaluar directa (pérdida de dinero) o indirectamente (productividad e imagen reputacional) el impacto al negocio. Para concluir, la identificación de las aplicaciones críticas no solo con un enfoque tecnológico sino al valor que genera para el negocio.

III. METODOLOGÍA

El enfoque de la presente investigación fue cualitativa porque tiene por objetivo entender y describir las experiencias de los participantes y el contexto que lo rodea, por otra parte, la recolección de los datos es realizada por el investigador, el cual es soportado por diversas herramientas que se van ajustando conforme se avanza con el estudio. Hernández y Mendoza (2018). Por otro lado, el paradigma de investigación fue interpretativo porque se busca comprender, recopilar y profundizar el conocimiento de acuerdo a la interpretación de los participantes. Hernández y Mendoza (2018).

3.1. Tipo y diseño de investigación

Tipo de investigación

La presente investigación fue básica, porque se busca descubrir o ampliar los conocimientos del estándar de seguridad para la protección de los datos de las tarjetas de pago. Ñaupa (2014). Por otro lado, Hernández y Mendoza (2018) indicaron que, en una investigación básica surge la necesidad de la búsqueda de conocimientos o soluciones con la finalidad de enriquecer la teoría ya existente sobre el tema de estudio.

Diseño de investigación

En el presente trabajo se utilizó el diseño investigación acción, debido a que se busca mejorar la seguridad de las tarjetas de pago a través de un estándar de seguridad que permita reducir el riesgo de acceso no autorizado a la información de los tarjetas habientes, para ello se requiere implementar una solución holística de seguridad entre los diferentes dispositivos tecnológicos y los clientes para reducir la materialización de los ataques tanto físicos como desde la nube. Hernández y Mendoza (2018).

3.2. Categorías, Subcategorías y matriz de categorización

Las categorías como la disponibilidad, confidencialidad, integridad y acuerdos de nivel de servicio componen el tema de investigación debido a que se utilizan para describen y entender sus características.

De igual manera, como parte de las investigaciones tanto la seguridad como la arquitectura tecnológica juegan un papel predominante en el desafío de reducir el riesgo de un ataque cibernético que perjudique a los clientes y a la entidad financiera, es por eso que desde un punto de vista holístico he señalado que las sub categorías como la configuración de firewall, contraseñas robustas, DRP, la protección de almacenamiento, cifrado, restricción de acceso físico, antivirus, aplicaciones seguras, asignación de acceso, mantenimiento preventivo, correcto y el BIA son los ejes para una correcta ejecución de los servicios bancarios en referencia a los tarjetas habientes. También es importante destacar que sin los mecanismos legales y regulatorios, como por ejemplo la súper intendencia de banca y seguros sería más compleja la implementación de estándares de seguridad. Resumiendo, se ha desagregado dichos procesos en categorías y sub categorías tal como lo indica la Tabla 1.

Tabla 1

Categorías y sub categoría de la investigación

Categorías	Sub categorías
Disponibilidad	▪ Configuración de firewall ▪ Contraseñas robustas ▪ Plan de recuperación de desastre
Confiabilidad	▪ Protección de almacenamiento de datos ▪ Cifrado de datos ▪ Restringir al acceso físico a los datos
Integridad	▪ Antivirus ▪ Aplicaciones seguras ▪ Asignación de acceso a los componentes del sistema
Acuerdos de nivel de servicios	▪ Mantenimiento preventivo ▪ Mantenimiento correctivo ▪ Análisis de impacto del negocio

3.3. Escenario de estudio

Se escogió como ubicación de estudio el área de tecnología, esta, se encuentra dentro de un edificio de 5 pisos, los cuales está distribuido en diferentes áreas administrativas y de soporte, cada piso tiene un cuarto de comunicaciones el cual permite la interconexión con las sedes internas y con entidades externas. El personal de tecnología está compuesto por tres pilares, el área de infraestructura el cual se subdivide entre la división de servidores y de telecomunicaciones; el área de servicios tecnológicos, el cual se subdivide entre la división de mesa de ayuda y de operación; el área de desarrollo, el cual se subdivide entre la división de aplicaciones CORE y aplicaciones satélites y por último el área de planeamiento, el grupo humano está compuesto por personal de experiencia en el sector bancario con trayectorias en promedio de 15 años. Debido a la pandemia, el 96% de los colaboradores está trabajando desde casa.

3.4. Participantes

La unidad de estudio es el área de tecnología, el cual está compuesto por las unidades de desarrollo e infraestructura, estos últimos participan en el proceso de arquitectura tecnológica y son los responsables de diseñar e implementar los mecanismos más adecuados a nivel de hardware y software que soportan los canales electrónicos tanto dentro como fuera de las instalaciones. Los participantes son expertos en configuraciones de base de datos, en implementación de MIDDLE WARE, en aplicaciones en la nube, configuraciones en equipos de comunicación tanto LAN como WAN, equipos de seguridad y administración de proyectos, por otra parte, se encargan de monitorizar todos los eventos categorizados como críticos para el negocio con la finalidad de asegurar el correcto comportamiento del servicio a través de herramientas de última generación para contar con la información más oportuna.

3.5. Técnicas e instrumentos de recolección de datos

Según Hernández y Mendoza (2018) indicaron que, el principal objetivo de la recolección es obtener datos como por ejemplo de creencias, emociones y pensamientos que finalmente y que a través de procesos homologados se convertirá en información, por otra parte, esta, tiene por finalidad analizar y comprender los datos con el propósito de responder a las preguntas de investigación y generar conocimiento. Existen distintas técnicas sin embargo para la presente investigación se utilizó la técnica de observación que tuvo por finalidad describir y profundizar los procesos relacionados con el objeto de estudio, la entrevista semiestructurada se utilizó para recopilar información de expertos de acuerdo al tema de investigación para comprender y ampliar los conocimientos y el análisis documental permitió ordenar y sintetizar los documentos originales para un mejor entendimiento del tema. Estas tres técnicas me sirvieron para entender y comprender nuevos conocimientos como por ejemplo categorías y subcategorías emergentes desde distintos observadores con la finalidad de enriquecer el trabajo de investigación y como instrumentos se utilizará la guía de observación, la guía de entrevista y la ficha de análisis documental.

3.6. Procedimientos

El procedimiento seguido para la entrevista semiestructurada consistió en coordinar y entrevistar a tres ingenieros en sistemas, especialistas en el rubro de seguridad de la información, con más de 10 años de experiencia en las áreas de tecnología y que estén trabajando en organizaciones afines o de consultoría lo que nos permite tener información creíble y fiable acerca de la seguridad y arquitectura de las tarjetas de pago, estas preguntas permiten recopilar y procesar de manera anónima mediante el análisis de triangulación para concluir con los resultados. El siguiente procedimiento fue el uso del instrumento de la observación que consistió en seleccionar tres personas del área de estudio involucradas directamente con la implementación de los dispositivos electrónicos y aplicaciones que están relacionadas con la implementación de mecanismos de seguridad en tarjetas de pago con la finalidad de determinar las mejoras que se deben de implementar.

3.7. Rigor científico

La presente investigación ha sido respetuoso de los criterios del rigor científico, utilizando las técnicas e instrumentos adecuados para la recopilación de los datos y su interpretación con la finalidad de otorgar credibilidad y validez a la investigación. Asimismo, la utilización de las revistas indexadas para los trabajos previos y el marco teórico permitió la confiabilidad de la información, por otro lado, el conocimiento del investigador en el área de estudio ha permitido la adecuada selección de los tres expertos para las entrevistas, los tres participantes para la observación y la selección de los documentos para el análisis documental. Adicionalmente, la honorabilidad del investigador permitió la rigurosidad científica a la investigación. Según Hernández y Mendoza (2018), indico que, una de las características de un trabajo de investigación cualitativa es que el trabajo de investigación debe de ser de calidad que tiene por finalidad determinar una serie de criterios como la confiabilidad, la validez y la objetividad, por otra parte, estos criterios se aplican tanto para el proceso como para el producto, dentro de ellos tenemos la credibilidad, que significa recopilar las experiencias de los participantes; la aplicabilidad, el cual tiene por objetivo trasladar el caso de estudio hacia otro contexto con la finalidad de ejecutar soluciones en otras ubicaciones, seguidamente la confirmación, el cual implica, rastrear los datos de las fuentes y explicar su interpretación.

3.8. Método de análisis de la información

El análisis de la información que se realizó en el presente trabajo de investigación, consistió en recolectar datos y aplicar el método llamado triangulación a la entrevista con el objetivo de corroborar los resultados y descubrimientos con la finalidad de darle mayor validez al estudio, de acuerdo Hernández y Mendoza (2018) indicaron que, la elección del método depende del planteamiento del problema y cada problema tiene una forma distinta de resolverla además permite enriquecer la muestra al tener varios enfoques, tener una mejor validez de los datos, incremento en la confiabilidad con la finalidad de tener una mejor perspectiva de los datos.

Para poder realizar el proceso de triangulación, primero, se utilizó la matriz de desgravación que consiste en registrar las respuestas de los tres especialistas; luego se desarrolló la matriz de codificación de la entrevista, que consiste en la selección de palabras claves de las respuestas previamente registradas en la matriz anterior, para terminar, se desarrolló una matriz de entrevistados y conclusiones el cual consolida todas las codificaciones por especialista para determinar su similitud o diferencia para luego finalmente llegar a una conclusión por parte del investigador para contar con un conocimiento más sólido sobre el caso de estudio.

3.9. Aspectos éticos

El presente trabajo se realizó de acuerdo a la resolución emitida por la Universidad Cesar Vallejo número 011, el código de ética del posgrado, el turnitin y el uso de la norma APA, por lo expuesto, el trabajo de investigación es original y no hace mención a la organización ni información confidencial, por otra parte tanto las técnicas como las entrevistas como la observación participativa fueron realizadas a personas de alta experiencia laboral y expertos sobre estándares de seguridad de tarjetas de pagos por cuanto las respuestas obtenidas son confiables y objetivas, mismas que se mantuvieron en anonimato de acuerdo a lo coordinado previamente con los especialistas.

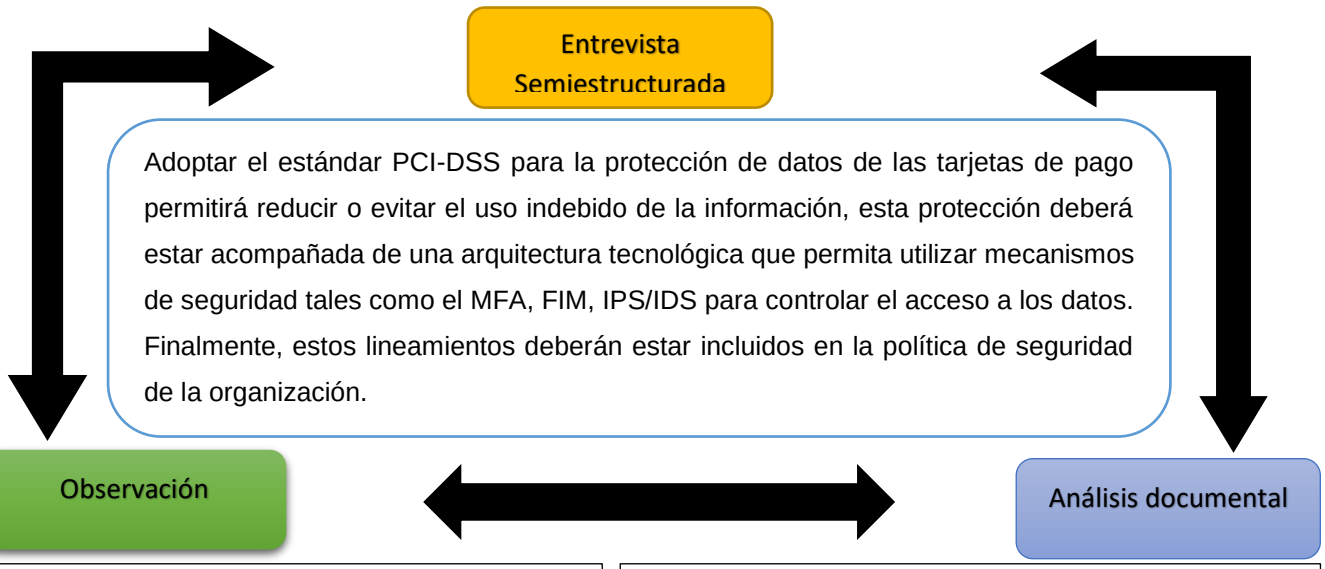
IV. RESULTADOS Y DISCUSIÓN

Para la presente investigación, los resultados han sido obtenidos con técnicas de recolección de datos, como la entrevista semiestructurada, observación y análisis documental, con la finalidad de cumplir los objetivos planteados. A continuación se muestra las distintas conclusiones de acuerdo al tipo de triangulación.

Figura 5

Triangulación de las técnicas de investigación utilizadas

Se concluye, que para la protección de los datos de las tarjetas de pago se debe de tener en cuenta tres pilares de seguridad, los cuales son, la disponibilidad, la confidencialidad e integridad de los datos, por otra parte, la arquitectura tecnológica juega un papel crucial debido a que se debe de tener en cuenta las características de los dispositivos electrónicos, sus configuraciones y la administración para el correcto funcionamiento de los servicios. Finalmente es fundamental contar con los lineamientos y políticas de seguridad claros para determinar el tratamiento de la información, como es el caso de cifrar los datos y restringir los accesos para reducir ataques como denegación de servicio y fuga de información que signifiquen accesos no autorizados.



Se concluye que para la protección de los datos de las tarjetas de pago se tiene que diseñar una arquitectura tecnológica que permita cubrir los tres pilares de seguridad como son la disponibilidad, confidencialidad e integridad de los datos, por otra parte, observo que cuentan con los mecanismos de seguridad a nivel de infraestructura y procedimientos que permiten el aseguramiento de los datos sin embargo, si es necesario realizar algunas mejoras a nivel funcional y técnico, como por ejemplo, bloquear la tarjeta de pago, desactivar funciones de compras por internet desde la aplicación móvil y finalmente, coordinar con las entidades a fines para la masificación del lector por CHIP en vez de banda magnética para aumentar la seguridad de las operaciones financieras.

Se concluyó que los mecanismos de seguridad que se deben de implementar deben de estar enfocados en la protección de datos de las tarjetas de pagos tanto dentro como fuera de la organización de la red y que estás medidas deben de estar normadas en una política de seguridad para su aplicación, actualización y monitoreo. Adicionalmente, contar con un plan de capacitación que permita informar a los colaboradores de los riesgos y fraudes que podrían estar expuestos en caso de no seguir los lineamientos de seguridad.

Al triangular las tres técnicas se concluye que, adoptar el estándar de seguridad PCI-DSS para la protección de datos de las tarjetas de pago permitirá reducir o evitar el uso indebido de la información, esta protección deberá estar acompañada de una arquitectura tecnológica que permita utilizar mecanismos de seguridad tales como el MFA, FIM, IPS/IDS y el factor humano para controlar el acceso a los datos con la finalidad de asegurar la disponibilidad, la integridad y la confiabilidad de la información de los tarjetas habientes, esta estrategia deberá estar incluida en la política de seguridad de la organización. Por otra parte, Thomas et al (2020), nos indica, que para reducir alteraciones o modificaciones en los datos es imprescindible implementar protocolos seguros como es el caso del HTTPS, SSH o SFTP. Yeh et al. (2020) sostuvo que, la operadora de tarjetas de pago visa utiliza un modelo llamado multimodal que no es más que un método de auto aprendiza para detectar los fraudes, la técnica es no solo generar patrones individuales por tienda comercial o por consumidor sino más bien por afinidad para mejor el nivel de acierto, la identificación comerciante-consumidor es importante para garantizar la integridad del procesamiento de pagos. Balagolla et al. (2021) afirmó que con la rápida expansión de las transacciones, la globalización tecnológica ha impulsado el uso de tecnologías emergentes como la Blockchain para la gestión de tarjetas de pago, bancos como JP Morgan, HSBC, BBVA, Santander y el BCP ya están en el proceso de usar Blockchain para el intercambio de transacciones financieras sin importar la ubicación física del cliente, esto permitirá reducir que la información sea alterada debido a la descentralización del procesamiento. Esta conclusión responde al objetivo específico que consiste en determinar la integridad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras. Finalmente, los mecanismos de seguridad se detallan en la tabla 2

Tabla 2

Mecanismos de seguridad para reducir alteraciones de la información

Mecanismos	Descripción
Implementar el MFA (Multi Factor de autenticación)	• Acceso a las aplicaciones con doble autenticación • Registro de auditoria.
IDS/IPS	• Detectar ataques • Prevenir de ataques
FIM (File Integrity Monitoring)	• Registro de ataques • Monitoreo de cambios en archivo
Factor humano	• Capacitación • Concientización organizacional • Gestión de perfiles de usuarios

Por otro lado, de acuerdo a las entrevistas semiestructurada que se aplicó a los tres expertos en seguridad de la información, se identificó algunas categorías y subcategorías emergentes, tal como se indica en la Tabla 3

Tabla 3

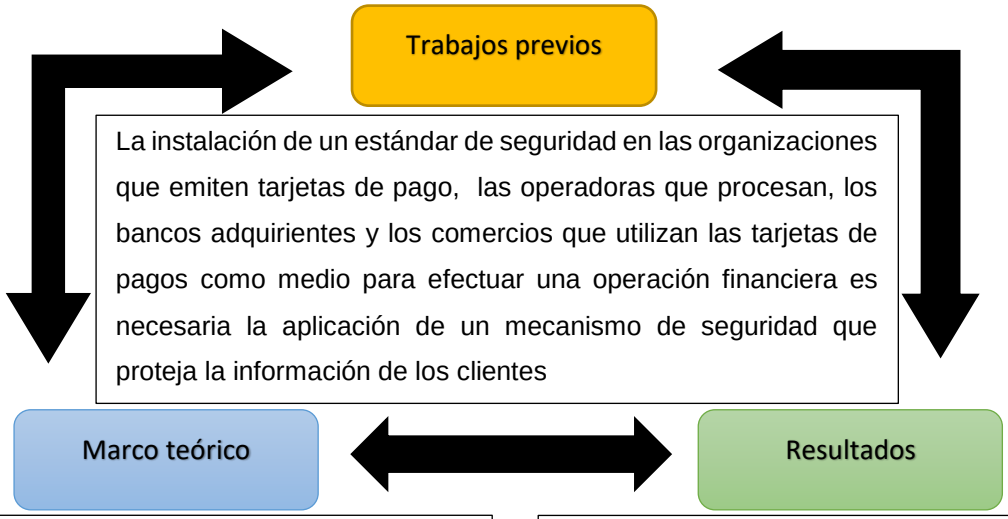
Categorías y subcategorías emergentes

Categorías	Subcategorías
• ISO 27001 • PCI-CP • Factor humano • FIM	• Revisión cruzada • Cultura organizacional • Listas blancas • Need to Know

Figura 6

Triangulación de trabajos previos, marco teórico y resultado

Albornoz et al (2017) indica que, el 75% de las personas encuestadas no usa la banca móvil debido a la falta de seguridad en las operaciones financieras y que para reducir este riesgo es requerido la implementación del estándar PCI-DSS. Chaithanya et al (2021) quien concluyó que, para reducir el fraude en las transacciones financieras es necesario la implementación de dispositivos biométricos como la huella digital para evitar el transporte de la tarjeta en físico



Se concluye, que el estándar de seguridad PCI-DSS permite proteger los datos de aquellas transacciones financieras que trasmiten, procesan o almacenan información de las tarjetas de pago y que los escáneres de seguridad de la industria no contemplan al 100% de las vulnerabilidades registradas por el estándar.

Se concluye que, adoptar el estándar de seguridad PCI-DSS para la protección de datos de las tarjetas de pago permitirá reducir o evitar el uso indebido de la información, esta protección deberá estar acompañada de una arquitectura tecnológica que permita utilizar mecanismos de seguridad tales como el MFA, FIM, IPS/IDS y el factor humano para controlar el acceso a los datos con la finalidad de asegurar la disponibilidad, la integridad y la confiabilidad de la información de los tarjetas habientes. Adicionalmente, estos lineamientos deberán estar incluidos en la política de seguridad de la organización.

Se concluye que para reducir el fraude cibernético en cualquier canal electrónico se requiere de la aplicación del estándar de seguridad PCI-DSS, PCI-CP, ISO27001 y de un sistema de inteligencia artificial como Machine Learning y biometría tanto en las organizaciones emisoras que emiten tarjetas de pago, las operadoras que procesan las transacciones financieras, los bancos adquirientes y los comercios para salvaguardar la información del cliente. El Madhoun.et al. (2020) precisó que, la comunicación entre el punto de venta y la tarjeta de pago del cliente debe de estar asegurada mediante mecanismos de encriptación como el protocolo EMV ya que la transacción almacena datos sensibles. Sheng et al. (2011) sostuvo que, una manera menos costosa de asegurar rendimiento y seguridad es la implementación de BIFS (Bit-Interleaving File System) el cual permite que los datos estén divididos en varias ubicaciones físicas de almacenamiento para mantener la privacidad de los datos sin encarecer la seguridad y el rendimiento tecnológico. Yeh et al. (2020) concluyó que, la operadora de tarjetas de pago visa utiliza un modelo llamado multimodal que es más que un método de auto aprendiza para detectar los fraudes, la técnica es no solo genera patrones individuales por tienda comercial o por consumidor sino más bien por afinidad para mejor el nivel de acierto, la identificación comerciante-consumidor es importante para garantizar la integridad del procesamiento de pagos. Esta conclusión responde al objetivo general que consiste en proponer la implementación de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras tal como también se indica en la tabla 4.

Tabla 4

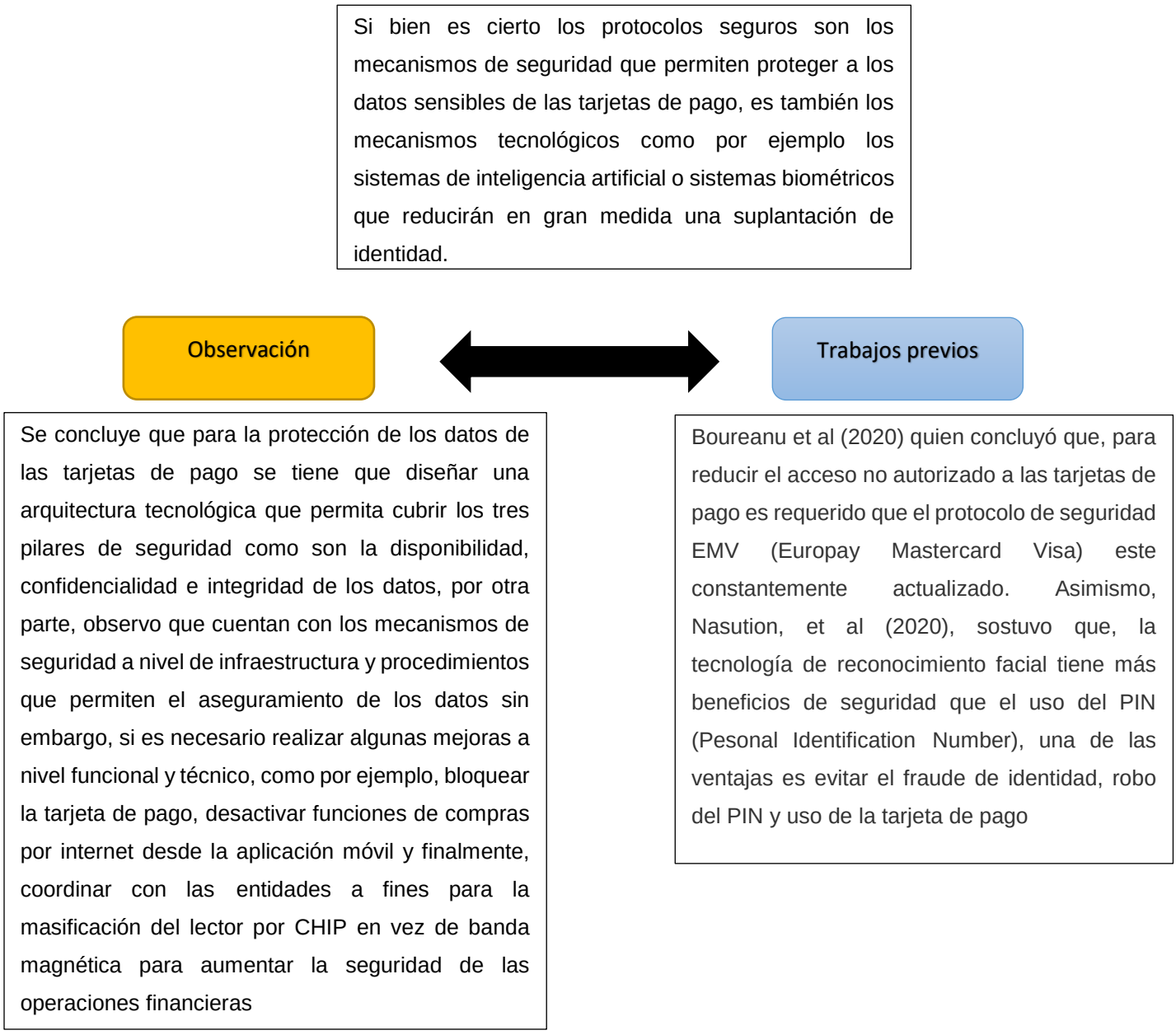
Estándares de seguridad para la protección de datos de tarjetas de pago

Estándares	Descripción
PCI-DSS	Payment Card Industry Data Security Standard, permite proteger la información sensible de las tarjetas de pago
PCI-CP	Payment Card Industry Card Production, definen los criterios de

	seguridad física y lógica que deben ser implementados durante los procesos de producción y el suministro de tarjetas de pago.
ISO 27001	Encargada de emitir los lineamientos de seguridad en la organización.
Biometría	Reconocimiento de huella dactilar, facial y de retina acompañado de una arquitectura tecnológica que lo soporte
Machine Learnig	Sistemas informáticos que permiten el autoaprendizajes de patrones de comportamientos
BIFS (Bit-Interleaving File System)	Es una arquitectura que permite distribuir los datos en distintos almacenamientos para el endurecimiento del acceso.
Autenticación por doble factor de autenticación (2FA)	Este estándar permite tener acceso a la información a través de una doble autenticación usando un código SMS, una llamada telefónica o de una llave aleatoria.
Geolocalización	Es un estándar que permite triangular entre el teléfono móvil y la tarjeta de pago su ubicación para realizar la transacción.

Figura 7

Triangulación de observación y trabajos previos



Se concluye que, para mitigar el acceso a los datos sensibles de las tarjetas de pago es necesario la implementación del protocolo EMV (Europay Mastercard Visa), cambiar la arquitectura de banda magnética por CHIP, controlar el acceso físico a los dispositivos electrónicos, cifrar datos activos/reposo, capacitación, contar con un programa de Ethical Hacking, uso de código seguro y finalmente la

implementación de inteligencia artificial sobre la gestión de tarjetas de pago tanto en la red interna como en la red externa. Asimismo, Daud et al. (2018), concluyó que, el cifrado de datos permite asegurar la confidencialidad de la información de punto a punto a través de protocolos como AES, 3DES o DES Esta conclusión responde al objetivo específico de la investigación que consiste en determinar la confidencialidad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, sobre este enfoque, los especialistas han dado respuesta al objetivo, tal como lo indica en la Tabla 5.

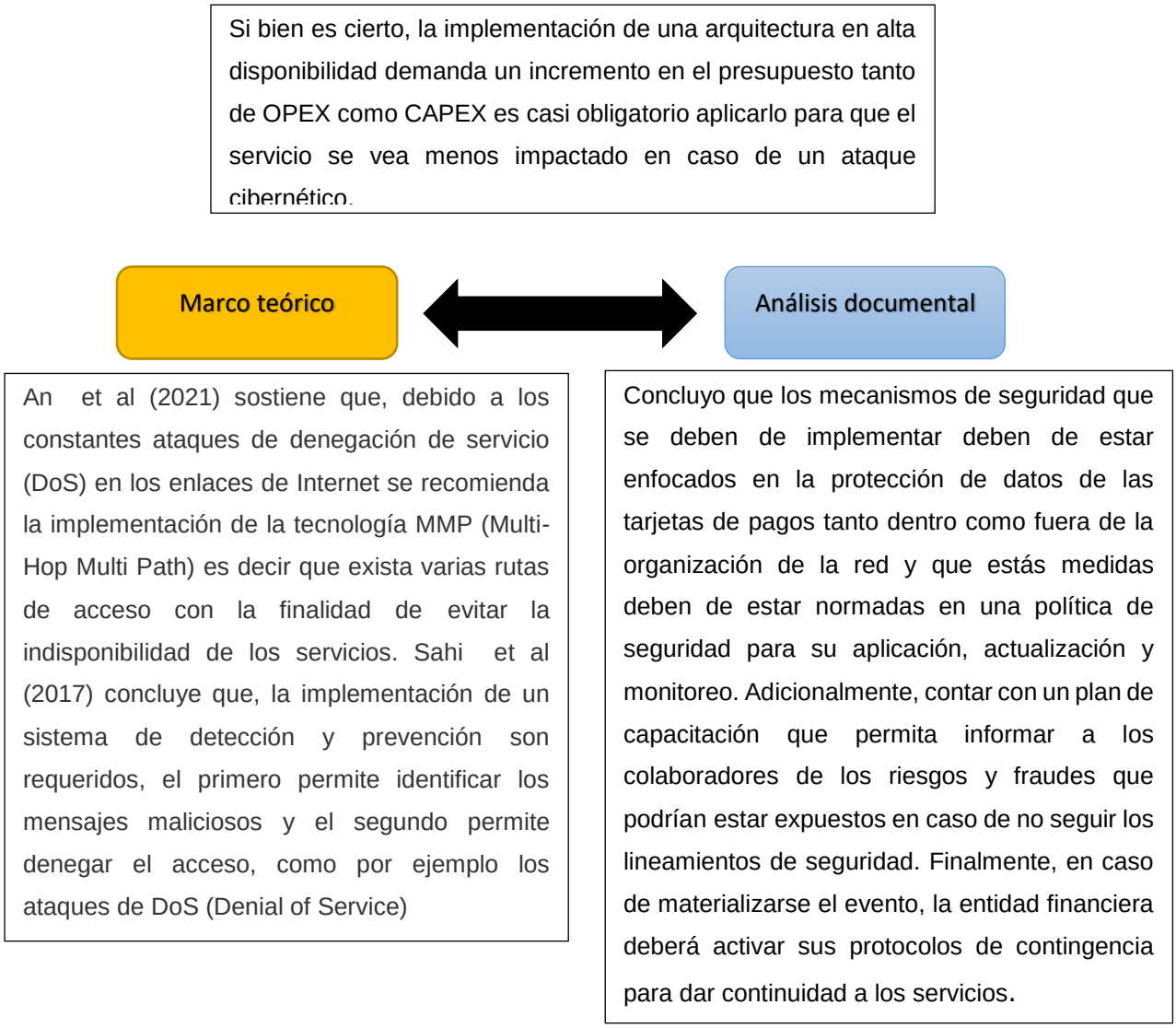
Tabla 5

Mecanismos para controlar el acceso a los datos

Mecanismos	Descripción
Hardware	• Implementación de CHIP en las tarjetas de pago • Controles físicos en los dispositivos electrónicos
Software	• Cifrar datos activos y en reposo • Especificar perfiles de usuarios • Ejecutar el proceso de Ethical Hacking de forma periódica • Uso de técnicas de código seguro • Capacitación de ataques cibernéticos

Figura 8

Triangulación de marco teórico y análisis documental



Se concluye que la arquitectura tecnológica que conforma los dispositivos electrónicos y datos de las tarjetas de pago puedan proteger la información de los tarjetas habientes se debe diseñar una arquitectura en alta disponibilidad tanto a nivel de red como en equipos microinformáticos, asignar un presupuesto tanto de OPEX como CAPEX, contar un DRP (Disaster Recovery Planning), actualización de parches de seguridad y llevar un control de cambios en la infraestructura para el acceso y protección oportuna, con la finalidad de que el servicio se vea menos impactado ante un ataque cibernético.

Asimismo, Chowdhury et al. (2020) indicó que, el fraude sigue siendo uno de los factores principales de pérdidas financieras de servicios en línea, es por ese motivo que para reducir el acceso no autorizado en Bangladesh, se implementó 6 tipos de contraseñas heurísticas como ejemplo, guías para la construcción de las contraseñas, mecanismo para la recuperación de contraseñas, utilización de CATCHA, preguntas de seguridad, utilización de HTTPS y medidor de contraseña. Esta conclusión responde al objetivo específico que consiste en determinar la disponibilidad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, tal como también se indica en la Tabla 6.

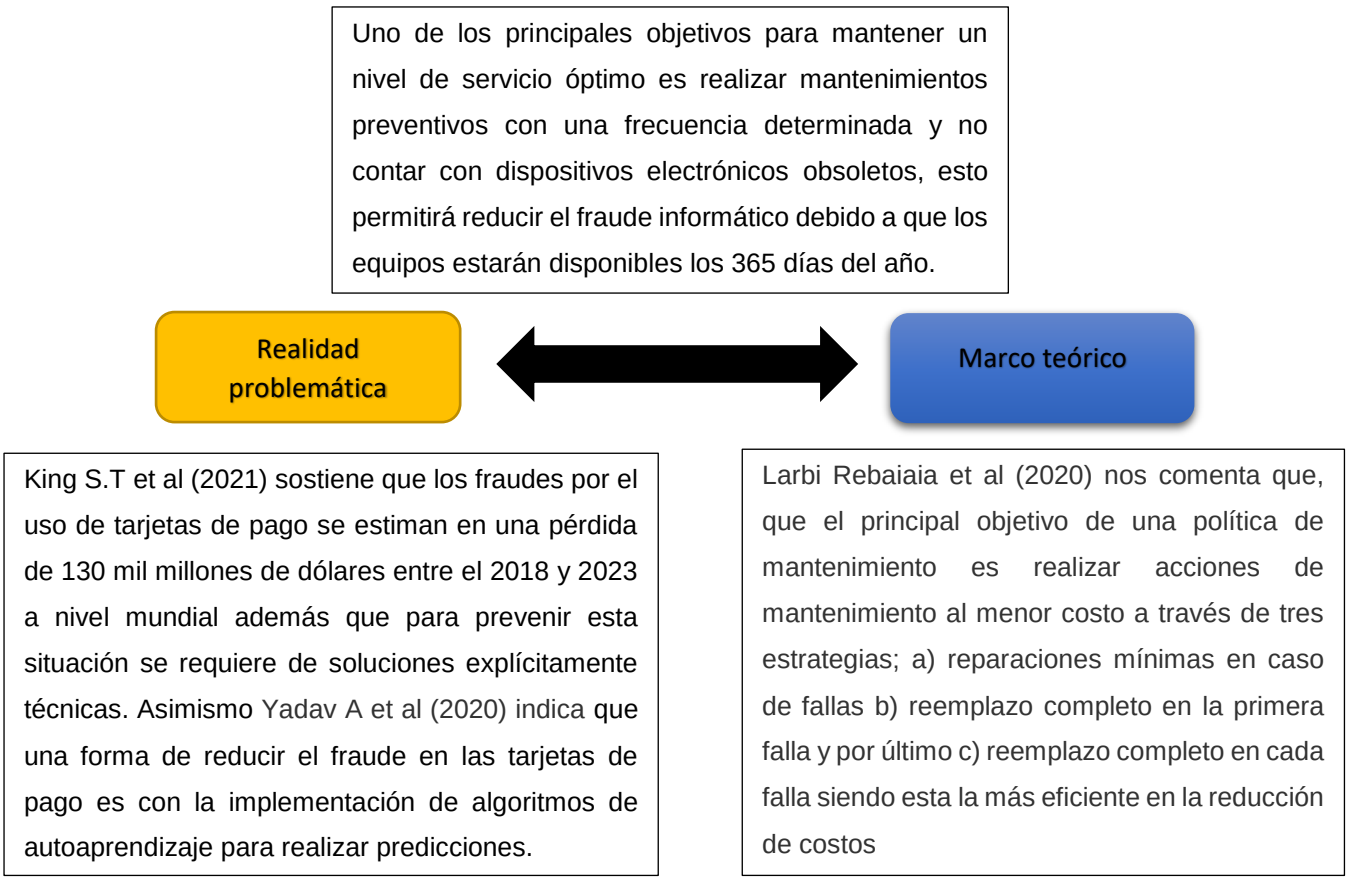
Tabla 6

Pilares de la disponibilidad a nivel de seguridad

Alcance	Descripción
Hardware	• Implementación de equipos de seguridad • Adquisición de equipos para DRP
Software	• Actualización de parches • Actualización de base de datos de antivirus
Documentación	• Controles de cambios • Segmentación de RED

Figura 9

Triangulación de la realidad problemática y marco teórico



Se concluye que para mantener un nivel de servicio óptimo se debe de realizar mantenimientos preventivos con periodicidad, monitoreo a través de tableros de control y no contar con dispositivos electrónicos obsoletos o fuera de soporte de proveedor y de fábrica, esto permitirá reducir el fraude informático debido a que los equipos estarán disponibles los 365 días del año. Lai et al. (2019) concluyó que los mantenimientos correctivos tradicionales están siendo reemplazados por los CBM (Condition base maintenance) a través del IoT con la finalidad de mejorar la seguridad y confiabilidad de los equipos tecnológicos es decir prolongando su vida útil, reduciendo incidentes e interrupciones al negocio de una manera más predictiva mediante la recopilación, análisis de los datos y la toma de decisiones. Esta conclusión da respuesta al objetivo específico que consiste en determinar los

acuerdos de nivel de servicio en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago, más detalle en la tabla 7.

Tabla 7

Acuerdos y tableros de control de niveles de servicio

Alcance	Descripción
Contratos	• Mantenimiento preventivos • Mantenimientos correctivos • Penalidades
Acuerdos d nivel de servicios	• Indicadores de rendimiento • Monitoreo de indicadores e incidentes • Definición de métricas

V. CONCLUSIONES

PRIMERA:

En relación del objetivo general, se concluye que para reducir el fraude cibernético en cualquier canal electrónico se requiere de la aplicación del estándar de seguridad PCI-DSS, PCI-CP, ISO27001 y de un sistema de inteligencia artificial como Machine Learning y biometría tanto en las organizaciones emisoras que emiten tarjetas de pago, las operadoras que procesan las transacciones financieras, los bancos adquirientes y los comercios para salvaguardar la información del cliente

SEGUNDA:

En relación al primer objetivo específico, se concluye que la arquitectura tecnológica que conforman los dispositivos electrónicos y datos de las tarjetas de pago puedan proteger la información de los tarjetas habientes, se debe de diseñar una infraestructura en alta disponibilidad tanto a nivel de red como en equipos microinformáticos, asignar un presupuesto tanto de OPEX como CAPEX para la adquisición o renovación de equipos informáticos, contar un DRP (Disaster Recovery Planning), actualización de parches de seguridad y llevar un registro y gestión de los cambios realizados en la infraestructura para contar con el acceso 24x7 y protección oportuna, con la finalidad de que el servicio se vea menos impactado ante un ataque cibernético

TERCERA:

En relación del segundo objetivo específico, se concluye que, para mitigar el acceso a los datos sensibles de las tarjetas de pago es necesario la implementación del protocolo EMV (Europay Mastercard Visa), cambiar la arquitectura de banda magnética por CHIP, controlar el acceso físico a los dispositivos electrónicos, cifrar datos activos/reposo, capacitación, contar con un programa de Ethical Hacking, uso de código seguro y finalmente la implementación de inteligencia artificial sobre la gestión de tarjetas de pago tanto en la red interna como en la red externa

CUARTA:

En relación al tercer objetivo específico, se concluye que, adoptar el estándar de seguridad PCI-DSS para la protección de datos de las tarjetas de pago permitirá reducir o evitar el uso indebido de la información, esta protección deberá estar acompañada de una arquitectura tecnológica que permita utilizar mecanismos de seguridad tales como el MFA, FIM, IPS/IDS y el factor humano para controlar el acceso a los datos con la finalidad de asegurar la disponibilidad, la integridad y la confiabilidad de la información de los tarjetas habientes, esta estrategia deberá estar incluida en la política de seguridad de la organización

QUINTA:

Se concluye que para mantener un nivel de servicio óptimo se debe de realizar mantenimientos preventivos con periodicidad, monitoreo a través de tableros de control y no contar con dispositivos electrónicos obsoletos o fuera de soporte de proveedor y de fábrica, esto permitirá reducir el fraude informático debido a que los equipos estarán disponibles los 365 días del año

VI. RECOMENDACIONES

PRIMERA:

Se recomienda al responsable del área de tecnología realizar un análisis situacional de la infraestructura a nivel de hardware, software y aplicaciones del negocio para determinar los cambios que se deben de contemplar en el plan estratégico de tecnología de la información, por otra parte, coordinar con los socios de negocio tecnológicos para realizar un estudio de factibilidad para la utilización de sistemas biométricos, finalmente analizar la estructura de la información almacenada en las base de datos para la aplicación de herramientas con inteligencia artificial basados en patrones de comportamiento.

SEGUNDA:

Se recomienda al responsable del área de tecnología reemplazar los equipos informáticos obsoletos es decir aquellos que están fuera de soporte del fabricante, actualizar los equipos con el más reciente firmware de seguridad, implementar equipos en alta disponibilidad, contar con un centro de cómputo alterno con equipamiento replicado, realizar un análisis de riesgo para evaluar la criticidad de los equipos e identificar escenarios de fallas, crear indicadores de rendimiento para evaluar la salud de los equipos y mantener actualizado los procedimientos para saber los pasos a realizar en caso de indisponibilidad de algunos de los servicios.

TERCERA:

Se recomienda al responsable del área de tecnología contar con un plan y una bitácora de actualización del protocolo EMV para evitar que un atacante tenga acceso a la información por una debilidad del código, cifrar los datos que se trasmiten por la red, contar con un sistema de doble factor de autenticación biométrico para asegurar el acceso a los datos, finalmente implementar machine Learning para descubrir patrones de comportamiento y de afinidad de los datos.

CUARTA:

Se recomienda al responsable del área de tecnología para reducir alteraciones de los datos contar con una política de cifrado, autenticación y monitoreo a través de equipos de seguridad como el SDWAN, sistemas biométricos como el reconocimiento facial, huella dactilar o iris y del uso de machine Learning para evaluar el comportamiento del cliente, comportamiento de los dispositivos electrónicos y del uso de los datos con las aplicaciones CORE o líneas de comandos.

QUINTA:

Se recomienda al responsable del área de tecnología incluir en los contratos la aplicación del mantenimiento preventivo tanto a nivel de software como de hardware al menos una vez al año, monitorear la salud de los equipos de acuerdo a una periodicidad y contar con un seguro de reposición ante fallas físicas contar con equipos nuevos.

REFERENCIAS

ASBANC (1 de Junio 2021). Estadísticas del sector. https://bit.ly/2ZXpG9k

Ayo C.K, Mac-Eze C.M, Adebiyi A.A, Oni A, Okesola J.O, Odun-Ayo (2021). Developing a Multi-factor Authentication-based Cardless Electronic Payment System IOP Conference Series: Earth and Environmental, doi: 10.1088/1755-1315/665/1/012009

Ajay Chowdary, M., Kundan, M., & Viji Amutha Mary, A. (2019). Effective Credit Card Forgery Prevention Using Multilevel Authentication. IOP Conference Series: Materials Science and Engineering, 590, 012021. doi:10.1088/1757-899x/590/1/012021

Alemu, T., Bandyopadhyay, T., & Negash, S. (2015). Electronic Payment Adoption in the Banking Sector of Low-Income Countries. International Journal of Information Systems in the Service Sector, 7(4), 27–47. doi:10.4018/ijisss.2015100102

An, H., Na, Y., Lee, H., & Perrig, A. (2021). Resilience Evaluation of Multi-Path Routing against Network Attacks and Failures. Electronics, 10(11), 1240. doi:10.3390/electronics10111240

Albornoz, M, Vargas, D, Zarate, F y Zarazaga, T (2017) Plan de negocio de una plataforma de pago móvil para transferencias monetarias [Tesis de maestría, Universidad ESAN].

https://bit.ly/304qbyE

Arora, A., & Gosain, A. (2021). Intrusion detection system for data warehouse with second level authentication. International Journal of Information Technology, 13(3), 877–887. doi:10.1007/s41870-021-00659-1

Bielefeld S "Administrative burden and the Cashless Debit Card: Stripping time, autonomy, and dignity from social security recipients" Australian Journal of Public Administration, 2021, doi: 10.1111/1467-8500.12509

Banco central de reserva del Perú (21 de agosto del 2015). Medidas de seguridad en las tarjetas de crédito.

https://bit.ly/3BRFGqy

Benamara, N. K., Keche, M., Wellington, M., & Munyaradzi, Z. (2021). Securing E-payment Systems by RFID and Deep Facial Biometry 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA). doi:10.1109/caida51941.2021.9425175

Bestami Yuksel, B., Bahtiyar, S., & Yilmazer, A. (2020). Credit Card Fraud Detection with NCA Dimensionality Reduction, 13th International Conference on Security of Information and Networks. doi:10.1145/3433174.3433178

Bojjagani, S., Sastry, V. N., Chen, C.-M., Kumari, S., & Khan, M. K. (2021). Systematic survey of mobile payments, protocols, and security infrastructure. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-021-03316-4

Boureanu, I., Chen, L., & Ivey, S. (2020). Provable-Security Model for Strong Proximity-based Attacks: With Application to Contactless Payments. Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. doi:10.1145/3320269.3384748

BCRP (21 de Diciembre 2020). Digitalización e inclusión financiera. https://bit.ly/3bLMNpR

Busse, K., Tahaei, M., Krombholz, K., von Zezschwitz, E., Smith, M., Tian, J., & Xu, W. (2020). Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). doi:10.1109/eurospw51379.2020.000

Bataev, A. V. (2019). The Model of Assessing Economic Efficiency of Biometric ATMs. 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). doi:10.1109/eiconrus.2019.8657319

Chowdhury, A. A., Chowdhury, F., & Ferdous, M. S. (2020). A Study of Password Security Factors among Bangladeshi Government Websites. 2020 23rd International Conference on Computer and Information Technology (ICCIT). doi:10.1109/iccit51783.2020.93927

Calderón, M, Choquehuanca, L, Herrera, L y Rojas, R (2019) Factores que limitan la adopción de medios de pagos electrónicos: caso bodegas tradicionales [Tesis de maestría, Universidad de ESAN].

https://bit.ly/3bOTV4U

Daud, F. A., Ab Rahman, R., Kassim, M., & Idris, A. (2018). Performance of Encryption Techniques Using Dynamic Virtual Protocol Network Technology. 2018 IEEE 8th International Conference on System Engineering and Technology (ICSET). doi:10.1109/icsengt.2018.8606381

Dumsky, D. V., & Isaev, E. A. (2015). Data Centers for Physical Research. Physics Procedia, 71, 298–302. doi:10.1016/j.phpro.2015.08.330

El Madhoun, N., Bertin, E., Badra, M., & Pujolle, G. (2020). Towards more secure EMV purchase transactions. Annals of Telecommunications". doi:10.1007/s12243-020-00784-1

El Madhoun, N., Bertin, E., Badra, M., & Pujolle, G. (2020). Towards more secure EMV purchase transactions. Annals of Telecommunications. doi:10.1007/s12243-020-00784-1

El Peruano (27 de Setiembre 2021). Bancos: Tres desafíos para implementar inteligencia artificial.

https://bit.ly/3GYEoxx

E.M. S. W. Balagolla, W. P.C. Fernando, R.M. N. S. Rathnayake, M. J.M. R. P. (2021).Wijesekera, A. N. Senarathne y K. Y. Abeywardhana, Credit Card Fraud Prevention Using Blockchain, *6th International Conference for Convergence in Technology (I2CT),* 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9418192.

Feofilova, T., Radygin, E., Alekseeva, J., & Ivanov, F. (2019). Economic aspects of national security. Proceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy. doi:10.1145/3372177.3373346

Farfán, J (2015) Solución Monedero electrónico. Caso Startup Tecnología en Perú [Tesis de maestría, Universidad de Piura].

https://bit.ly/3GVDYIl

Georgieva, S., Markova, M., & Pavlov, V. (2019). Using neural network for credit card fraud detection. RENEWABLE ENERGY SOURCES AND TECHNOLOGIES. doi:10.1063/1.5127478

Hernández, R. y Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. Ciudad de México, México: Edamsa Impresiones.

Hernández, R., Fernández, C. y Baptista, M. (2014). Metodología de la investigación. (6ta. ed.). México D.F., México.

https://bit.ly/2A1rWzf

Í. Erdoğan, O. Kurto, A. Kurt and Ş. Bahtıyar. (2020). A New Approach for Fraud Detection with Artificial Intelligence, 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302374.

King S.T., *Scaife N., Traynor P., Abi Din Z., Peeters C., Venugopala* H. (2021).Credit Card Fraud Is a Computer Security Problem", 2021 IEEE Security and Privacy, 19 (2) art. no. 9382389 pp. 65-69, doi: 10.1109/MSEC.2021.3050247

Krishna Chaithanya, J., Donesh, N., Chakri Sreedhar, S., Teja, N. S., & Alekya, K. S. (2021). Design and Development of Virtual Banking Using Internet of Things, 2021 6th International Conference on Communication and Electronics Systems (ICCES). doi:10.1109/icces51350.2021.9489258

Karrupusamy, P., Chen, J., & Shi, Y. (Eds.). (2020). Sustainable Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies. doi:10.1007/978-3-030-34515-0

Karrupusamy, P., Chen, J., & Shi, Y. (Eds.). (2020). Sustainable Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies. doi:10.1007/978-3-030-34515-0

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2018). ATM Card Cloning and Ethical Considerations. Science and Engineering Ethics. doi:10.1007/s11948-018-0049-x

Lainformacion (11 de Julio 2019) El Machine Learning ya es indispensable para el 90% de las financieras del mundo.

https://bit.ly/2YmPmeW

Larisa, G., Tetiana, N., & Viktoriia, V. (2019). Neobanks Operations and Security Features". 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). doi:10.1109/picst47496.2019.90612

Li, C., & Gaudiot, J.-L. (2019). Detecting Malicious Attacks Exploiting Hardware Vulnerabilities Using Performance Counters. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). doi:10.1109/compsac.2019.00090

Lai, C. T. A., Jiang, W., & Jackson, P. R. (2019). Internet of Things enabling condition-based maintenance in elevators service. Journal of Quality in Maintenance Engineering. doi:10.1108/jqme-06-2018-0049

Larbi Rebaiaia, M., & Ait-kadi Daoud. (2020). Maintenance policies with minimal repair and replacement on failures: analysis and comparison. International Journal of Production Research, 1–23. doi:10.1080/00207543.2020.1832275

Michael Yeh, C.-C., Zhuang, Z., Zheng, Y., Wang, L., Wang, J., & Zhang, W. (2020). Merchant Category Identification Using Credit Card Transactions. 2020 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata50022.2020.937

Meléndez, J (2020) Software OPELECT en máquina virtual y la prevención del riesgo del fraude electrónico de las operaciones bancarias de los clientes de Lima Metropolitana [Tesis de maestría, Universidad Nacional Federico Villareal].

https://bit.ly/3q8XqeS

Nasution, M. I. P., Nurbaiti, N., Nurlaila, N., Rahma, T. I. F., & Kamilah, K. (2020). Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic. 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE). doi:10.1109/ic2ie50715.2020.9274654

Nyarko-Boateng, O., Weyori, B. A., & Tetteh, L. A. (2020). Optimized Authentication Model for Online Transaction Payments. Journal of Computer Science, 16(2), 225–234. doi:10.3844/jcssp.2020.225.234

N, M., Thomas, A., S, I., & Bindhumadhava, B. S. (2020). A Traffic Monitoring and Policy Enforcement Framework for HTTP. 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP). doi:10.1109/isea-isap49340.2020.235004

Ñaupas, Mejía, Novoa y Villagómez. (2013). Metodología de la Investigación Cuantitativa y Cualitativa, 3° Edición, Ediciones de la U. Perú

Radkov, R. S., & Dimitrov, I. D. (2018). Are Disaster Recovery Levels sufficient to assess the Data Center's disaster preparedness? 2018 IEEE XXVII International Scientific Conference Electronics - ET. doi:10.1109/et.2018.8549602

Rahaman, S., Wang, G., & Yao, D. (Daphne). (2019). Security Certification in Payment Card Industry. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security - CCS '19. doi:10.1145/3319535.3363195

PwC's Global Economic Crime and Fraud Survey (2020) Fighting fraud A never-ending battle

Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021). "Time to Change the CVSS? IEEE Security & Privacy", 19(2), 74–78. doi:10.1109/msec.2020.3044475

Sitek, A., & Kotulski, Z. (2020). A New Card-Linked Loyalty Program: Estimated and Anticipated Benefits for Payment Transaction Parties. Electronics, 9(11), 1956. doi:10.3390/electronics9111956

Samaranayake, C., Achchige, R. K., Shanaz, T., Ranasinghe, A., & Senarathne, A. (2019). "Enhanced Secure Solution for PoS Architecture". 2019 International Conference on Advancements in Computing (ICAC). doi:10.1109/icac49085.2019.910333

Saxena, S., Vyas, S., Kumar, B. S., & Gupta, S. (2019). Survey on Online Electronic Paymentss Security. 2019 Amity International Conference on Artificial Intelligence (AICAI). doi:10.1109/aicai.2019.8701353

Saia, R., & Carta, S. (2018). Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. Future Generation Computer Systems. doi:10.1016/j.future.2018.10.016

Sahi, A., Lai, D., Li, Y., & Diykh, M. (2017). An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment. IEEE Access, 1–1. doi:10.1109/access.2017.2688460

Sheng, Z., Ma, Z., Gu, L., & Li, A. (2011). A privacy-protecting file system on public cloud storage. 2011 International Conference on Cloud and Service Computing. doi:10.1109/csc.2011.6138512

Yadav A., Jain V, Kumar A. (2020). Performance analysis of machine learning algorithms in credit card fraud detection, 2020, Springer Science and Business Media Deutschland GmbH, doi: 10.1007/978-981-15-7345-3_26

Zhao, D., Luo, L., Yu, H., Chang, V., Buyya, R., & Sun, G. (2021). Security-SLA-guaranteed service function chain deployment in cloud-fog computing networks. Cluster Computing, 24(3), 2479–2494. doi:10.1007/s10586-021-03278-4

Anexo 1:

Matriz de categorización

Título: Estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021

Autor: Carlos Javier Montalvo Vivar

Problema General	Objetivo General	Categorías	Subcategorías	Técnicas	Instrumentos
¿Cuál es la situación actual de los estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?	Proponer la implementación de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021	Disponibilidad	▪ Configuración de firewall ▪ Contraseñas robustas ▪ Plan de recuperación de desastre	Entrevista Semi estructurada	Guía de Entrevista
Problemas Específicos	**Objetivos Específicos:**				
¿Cómo es la disponibilidad de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?	Determinar la disponibilidad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021	Confidencialidad	▪ Protección de almacenamiento de datos ▪ Cifrado de datos ▪ Restringir el acceso físico a los datacenters	Observación	Guía de observación
¿Cómo es la confidencialidad de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?	Determinar la confidencialidad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021				
¿Cómo es la integridad de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?	Determinar la integridad en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021	Integridad	▪ Antivirus ▪ Protocolos seguros ▪ Asignación de acceso a los componentes del sistema	Análisis documental	Ficha de análisis documental
¿Cómo es el acuerdo de servicio de estándares de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021?	Determinar los acuerdos de nivel de servicio en la implementación de estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021	Acuerdo de servicio	▪ Mantenimiento preventivo ▪ Mantenimiento correctivo ▪ Impacto de análisis de negocio		

Fuente: Rahaman (2019)

Anexo 2:

Instrumento de recolección de datos

1. ¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?
2. ¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?
3. ¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?
    a. ¿Qué lineamientos de seguridad se debería de contar en la configuración de firewall en la protección de las tarjetas de pago?
    b. ¿Qué características debe de tener una contraseña robusta?
    c. ¿Qué características debe tener el plan de recuperación de desastre?
4. ¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?
    a. ¿Qué mecanismos de seguridad se debe de implementar para la protección de los datos almacenados de las tarjetas de pago?
    b. ¿Cuál es el alcance que se debería considerar en el cifrado de datos?
    c. ¿Qué relación existe entre la protección de los datos de las tarjetas de pago con la restricción física de los datacenters?
5. ¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?
    a. ¿Qué características debería tener un antivirus para proteger los datos de las tarjetas de pago?
    b. ¿Cuál es la importancia de implementar protocolos seguros tanto en una red interna como externa?
    c. ¿Qué beneficios a nivel de seguridad se tiene en la asignación de acceso a los componentes del sistema?
6. ¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?
    a. ¿Qué consideraciones debería tener el mantenimiento preventivo en los equipos tecnológicos?
    b. ¿Qué características debe de tener el mantenimiento correctivo?
    c. ¿Cuál es la importancia del análisis de impacto al negocio?

Anexo 3:

Matriz de desgravación de entrevistas

N°	**Preguntas**	**Entrevistado 1** – Consultor Senior Internacional en seguridad de la información
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	La mejor estrategia para reducir el riesgo es primero identificar todos los dispositivos electrónicos que existe en la organización, determinar aquellos equipos que procesen, trasmitan y almacenen información para que finalmente se pueda depurar la mayor cantidad de equipos tecnológicos innecesarios. Luego de esta actividad se implementará los controles requeridos por el estándar PCI-DSS
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	Si bien es cierto PCI-DSS es un conjunto de estándares de seguridad consolidados de las marcas VISA, Master Card, American Express y Discover (Diners Club) existen otras más relacionadas a la protección de las tarjeas de pago, como por ejemplo; P2P (Peer to Peer) utilizado para pago de transacciones en línea, PIN Security es un estándar de seguridad que establece los requerimientos para la gestión segura, procesamiento y transmisión del número de identificación personal (PIN) durante el procesamiento de transacciones de pago en línea y fuera de línea en cajeros, APS (Application Package Standard) que se utiliza para el desarrollo de software, Seguridad de software, Seguridad física y el estándar de pagos sin contacto, todos estos mecanismos de seguridad se utilizan para la protección de las tarjetas de pago.

3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	Lo primero que se debe de proteger es el dato, la afectación de un dispositivo electrónico afecta más a la operatividad que a la misma seguridad debido a que luego del incidente se deberá poner en funcionamiento dicho recurso, por otra parte es importante tener los inventarios lo más actualizado posible con el nivel de detalle que permita la trazabilidad de los equipos, tal igual a una historia clínica, como por ejemplo actualizaciones de parches, control de cambios. Por otra parte, para reducir la probabilidad de fallas en el sistema, algunos estándares de seguridad indican colocar un firewall por cada dispositivo ya sea utilizando aplicaciones libres o aplicaciones especializadas además se recomienda activar todos los LOGs disponibles para su revisión. Adicionalmente existe la posibilidad de mantener contraseñas de más de 20 caracteres y robustas en vez de contraseñas débiles, fácilmente detectado. Los planes de DRP se deben de probar al menos una vez al año.
4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	La única manera de proteger los datos es cifrar además debe de existir el mínimo privilegio a través de perfiles lo que se denomina listas blancas, es más sencillo implementar listas blancas que listas negras por su nivel de protección, por otra parte, los controles físicos son indispensables para documentar el acceso de las personas a través de bitácoras, estas deben de ser claras y precisas y cámaras de seguridad para monitorear todos los movimientos dentro de los cuartos de comunicaciones. Adicionalmente se debe de implementar un análisis de vulnerabilidad de forma periódica a través de técnicas como el Ethical Hacking de

		cada uno de los dispositivos para evitar problemas en la operación. Por otra parte, se recomienda que los desarrolladores se les capaciten en las técnicas de códigos seguros y desarrollo de páginas WEB. Asimismo, para reducir puertas traseras en el código de programación es importante la revisión de los programas por expertos, de no ser así, la probabilidad de generarse incidentes es alta. Toda conexión realizada desde afuera se debe de realizar a través de VPN para asegurar la información de un punto a otro.
5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	Para reducir la alteración de la información es importante la implementación de la tecnología MFA (Multi Factor Authentication) el cual permite tener varias capas de seguridad en el proceso de autenticación. Por otro lado, se recomienda la instalación de los IDS/IPS para la protección de las redes externas e interna y FIM (File Integrity Monitoring) que es una tecnología que monitorea y detecta cambios en los archivos lo cual puede ser un indicador de un ataque o brecha.
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	Los acuerdos de nivel de servicio no necesariamente están relacionados con la protección de las tarjetas de pago es decir no está enfocado con la recuperación o indicadores de los servicios sino más bien en encontrar la causa que provoco el incidente de seguridad aunque por otro lado en caso se quiera determinar lo que realmente sucedió entonces se debería contratar los servicios de un análisis forense.

N°	**Preguntas**	**Entrevistado 2** – Auditor Senior en seguridad de la información
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	A nivel de auditoria debería haber una revisión cruzada entre transacciones financieras y las áreas contables para dar validez a la operación para ayudar a reducir los fraudes. Por otra parte, el uso de la técnica de Machine Learning ayudará a identificar patrones o comportamientos sin embargo debe de estar constantemente ajustada para evitar los falsos positivos. Por otro lado, los controles son importantes para enviar alertas en caso de un evento, los validadores también cobran importancia para determinar el tipo de consumo adquirido para saber si la transacción está siendo comprometida.
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	Considero que el uso de las técnicas como PCI-DSS, ISO 27001 e inclusive COBIT permitirá a las entidades financieras estar más alineadas a los mecanismos de seguridad para mantener la confidencialidad e integridad de los datos. A nivel de auditoria es importante identificar el control para reducir el riesgo.
3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	La disponibilidad está más asociada al uso del recurso tecnológico, es más importante la confidencialidad e integridad de los datos. La entidad financiera es la responsable de asegurar que las transacciones financieras se puedan ejecutar en cualquier momento.
4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	Es uno de los pilares más importantes, la restricción física no asegura una protección de los datos debido a que en su mayoría es digital en cambio el cifrado es importante para proteger la información de los clientes, por otra parte

		es importante tener alineados a todos los colaboradores de la organización. El factor humano es el más sensible en toda la cadena de la seguridad. Los ataques de ingeniería social son los más usados para la intrusión a los datos.
5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	La protección de los datos, es una suerte de trabajar en conjunto entre el antivirus, protocolos seguros, perfiles. Hay una técnica llamada NEED TO KNOW que significa tener acceso a aquello que requiera saber para el correcto funcionamiento de sus funciones. Es importe realizar certificaciones de los perfiles de los usuarios, estas revisiones deberían realizarse con alguna periodicidad para reducir fuga de información, robo de operaciones y operaciones sospechosas. Por otra parte, las revisiones de los LOGS también es parte de la seguridad para verificar que las personas se están autenticando desde sus propios equipos menores para reducir fraudes. Los niveles de acceso también son revisados por los procesos de auditoria y estos deberían ser revisados a través de herramientas para que sean direccionados a las diferentes áreas de las entidades financieras.
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	No tener un acuerdo de nivel de servicio llama al desorden ya que afectaría a la disponibilidad, sobre todo dar la tranquilidad a los clientes de acceder a su información, por otra parte a nivel de auditoria los SLA tanto con los proveedores como con la áreas usuarias para verificar si existen brechas. Estos SLA son ajustables de acuerdo a la realidad de cada organización o de lo que requiere el usuario para atender sus operaciones. Es importante revisar los

		acuerdos respecto a los BECHMARKING que ya están estipulados en el sector o seguir las buenas prácticas. El análisis de impacto es importante para determinar los procesos críticos para activar los servicios más prioritarios debido a que no todo se podrá levantar a la vez, esto tiene que estar alineado con las áreas usuarias para verificar si es factible activarlo en un determinado tiempo o en su defecto verificar si la infraestructura actual la soporta caso contrario se requería realizar inversiones. El BIA debe ser escalado y aprobado al más alto nivel. El BIA se debe de realizar de manera anual y es responsabilidad del área usuaria.

N°	**Preguntas**	**Entrevistado 3** – Information Policy and Planning Consultant
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	Las tarjetas de crédito se deben de rediseñar ya que el problema sigue siendo la autenticación. La gran diferencia entre los estados unidos y Perú es el nivel cultural en la administración de la tarjeta de crédito ya que la confianza es uno sus los pilares principales.
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	Inicialmente todas las empresas que procesaban las tarjetas de pago manejaban sus propios estándares tales como VISA, MASTERCARD, por otro lado, además la familia PCI-DSS también se encuentra PCI-CP (Card Production) quienes se encargan de la construcción de las tarjetas de crédito,

		adecuación del CHIP, etcétera. Por otro parte, también existen estándares para aplicaciones que sirven para realizar pagos entre las entidades financieras.
3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	Siempre se debe de contar con un firewall tanto fuera como dentro del perímetro y segmentar la red de tal manera de proteger todos los equipos que si son PCI, es importante que los servicios estén disponibles pero cara a la seguridad no guarda relación con la confidencialidad o integridad de las tarjetas de pago ya que no hay compromisos de datos, por otra parte, si los dispositivos electrónicos no están disponibles un atacante puede aprovechar en introducir un malware ya que podría no tener los mismos mecanismos de seguridad como en producción en caso de estar trabajando en DRP.
4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	La protección de las tarjetas de pagos se basa en mantener la confiabilidad de los datos desde que se crea hasta que se utiliza, es el ciclo de vida de las tarjetas de pago. Sino aseguras confiabilidad significa que los datos no están protegidos. Para la transmisión de datos es importante cifrar como por ejemplo usando el protocolo TLS y también los datos que están en reposo. La restricción del acceso físico reduce la fuga de la información y es una de las capas de seguridad.
5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	Para que alguien cambie los datos es porque hay una intencionalidad o sea manipulado sea interna o externa. La función del antimalware es detectar programas maliciosos ya sea instalado en las PC o servidores, aunque el reto

		de los fabricantes es detectar el día cero y que sean configuradas con solo las listas blancas.
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	Los acuerdos de nivel de servicio están orientado a los controles, no está directamente relacionado a la protección de datos de las tarjetas de pago a nivel de confiabilidad o integridad sin embargo es importante definir bien los indicadores y métricas. Se deben de contar con las herramientas necesarias para monitorear diferentes tipos de ataque.

Anexo 4:

Matriz de codificación de la entrevista

N°	**Preguntas**	**Entrevistado 1 -** Consultor Senior Internacional en seguridad de la información	**Entrevista 1 Codificada**
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	La mejor estrategia para reducir el riesgo es primero identificar todos los dispositivos electrónicos que existe en la organización, determinar aquellos equipos que procesen, trasmitan y almacenen información para que finalmente se pueda depurar la mayor cantidad de equipos tecnológicos innecesarios. Luego de	• Identificar todos los dispositivos electrónicos • Determinar los equipos que procesen, trasmitan y almacenen información

		esta actividad se implementará los controles requeridos por el estándar PCI-DSS	• Depurar los dispositivos electrónicos innecesarios • Implementar controles
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	Si bien es cierto PCI-DSS es un conjunto de estándares de seguridad consolidados de las marcas VISA, Master Card, American Express y Discover (Diners Club) existen otras más relacionadas a la protección de las tarjeas de pago, como por ejemplo; P2P (Peer to Peer) utilizado para pago de transacciones en línea, PIN Security es un estándar de seguridad que establece los requerimientos para la gestión segura, procesamiento y transmisión del número de identificación personal (PIN) durante el procesamiento de transacciones de pago en línea y fuera de línea en cajeros, APS (Application Package Standard) que se utiliza para el desarrollo de software, Seguridad de software, Seguridad física y el estándar de pagos sin contacto, todos estos mecanismos de	• PCI-DSS • P2P (Peer to Peer) • PIN Security • APS (Application Package Standard) • Seguridad software • Seguridad física • Estándar de pagos sin contacto

		seguridad se utilizan para la protección de las tarjetas de pago.	
3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	Lo primero que se debe de proteger es el dato, la afectación de un dispositivo electrónico afecta más a la operatividad que a la misma seguridad debido a que luego del incidente se deberá poner en funcionamiento dicho recurso, por otra parte es importante tener los inventarios lo más actualizado posible con el nivel de detalle que permita la trazabilidad de los equipos, tal igual a una historia clínica, como por ejemplo actualizaciones de parches, control de cambios. Por otra parte, para reducir la probabilidad de fallas en el sistema, algunos estándares de seguridad indican colocar un firewall por cada dispositivo ya sea utilizando aplicaciones libres o aplicaciones especializadas además se recomienda activar todos los LOGs disponibles para su revisión. Adicionalmente existe la posibilidad de mantener contraseñas de más de 20 caracteres y robustas en vez de contraseñas	• Inventarios actualizados • Actualizaciones de parches • Control de cambios • Firewall • Activación de LOGs • Contraseñas de más de 20 caracteres • Planes de DRP

		débiles, fácilmente detectado. Los planes de DRP se deben de probar al menos una vez al año.	
4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	La única manera de proteger los datos es cifrar además debe de existir el mínimo privilegio a través de perfiles lo que se denomina listas blancas, es más sencillo implementar listas blancas que listas negras por su nivel de protección, por otra parte, los controles físicos son indispensables para documentar el acceso de las personas a través de bitácoras, estas deben de ser claras y precisas y cámaras de seguridad para monitorear todos los movimientos dentro de los cuartos de comunicaciones. Adicionalmente se debe de implementar un análisis de vulnerabilidad de forma periódica a través de técnicas como el Ethical Hacking de cada uno de los dispositivos para evitar problemas en la operación. Por otra parte, se recomienda que los desarrolladores se les capaciten en las técnicas de códigos seguros	• Cifrar para proteger los datos • Mínimo privilegio a través de perfiles • Implementar listas blancas • Controles físicos • Bitácoras • Cámaras de seguridad • Análisis de vulnerabilidad • Capacitación de técnicas de código seguro • Revisión de los programas por expertos

		y desarrollo de páginas WEB. Asimismo, para reducir puertas traseras en el código de programación es importante la revisión de los programas por expertos, de no ser así, la probabilidad de generarse incidentes es alta. Toda conexión realizada desde afuera se debe de realizar a través de VPN para asegurar la información de un punto a otro.	
5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	Para reducir la alteración de la información es importante la implementación de la tecnología MFA (Multi Factor Authentication) el cual permite tener varias capas de seguridad en el proceso de autenticación. Por otro lado, se recomienda la instalación de los IDS/IPS para la protección de las redes externas e interna y FIM (File Integrity Monitoring) que es una tecnología que monitorea y detecta cambios en los archivos lo cual puede ser un indicador de un ataque o brecha.	• Implementar la tecnología MFA (Multi Factor Authentication) • Instalación de IDS/IPS • FIM (File Integrity Monitoring)
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	Los acuerdos de nivel de servicio no necesariamente están relacionados con la protección de las tarjetas de pago es decir no	• No está relacionado con la protección de las tarjetas de pago

		está enfocado con la recuperación o indicadores de los servicios sino más bien en encontrar la causa que provoco el incidente de seguridad aunque por otro lado en caso se quiera determinar lo que realmente sucedió entonces se debería contratar los servicios de un análisis forense.	• Enfocado en encontrar la causa del incidente • Análisis forense.

N°	**Preguntas**	**Entrevistado 2 -** Auditor Senior en seguridad de la información	**Entrevista 2 Codificada**
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	A nivel de auditoria debería haber una revisión cruzada entre transacciones financieras y las áreas contables para dar validez a la operación para ayudar a reducir los fraudes. Por otra parte, el uso de la técnica de Machine Learning ayudará a identificar patrones o comportamientos sin embargo debe de estar constantemente ajustada para evitar los falsos positivos. Por otro lado, los controles son importantes para enviar alertas en caso de un evento, los validadores también	• Hacer revisión cruzada entre las transacciones financieras y contables • Machine Learning ayudará a identificar patrones • Controles para enviar alertas en caso de un evento

		cobran importancia para determinar el tipo de consumo adquirido para saber si la transacción está siendo comprometida.	• Los validadores son importantes para determinar el tipo de consumo
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	Considero que el uso de las técnicas como PCI-DSS, ISO 27001 e inclusive COBIT permitirá a las entidades financieras estar más alineadas a los mecanismos de seguridad para mantener la confidencialidad e integridad de los datos. A nivel de auditoria es importante identificar el control para reducir el riesgo.	• PCI-DSS • ISO 27001 • COBIT
3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	La disponibilidad está más asociada al uso del recurso tecnológico, es más importante la confidencialidad e integridad de los datos. La entidad financiera es la responsable de asegurar que las transacciones financieras se puedan ejecutar en cualquier momento.	• Es más importante la confidencialidad e integridad • Las transacciones financieras se deben de ejecutar en cualquier momento

4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	Es uno de los pilares más importantes, la restricción física no asegura una protección de los datos debido a que en su mayoría es digital en cambio el cifrado es importante para proteger la información de los clientes, por otra parte es importante tener alineados a todos los colaboradores de la organización. El factor humano es el más sensible en toda la cadena de la seguridad. Los ataques de ingeniería social son los más usados para la intrusión a los datos.	• La restricción física no asegura la protección de los datos • El cifrado protege la información • Todos los colaboradores de la organización deben de estar alineados • El factor humano es el más sensible en toda la cadena de la seguridad • Ingeniería social es el más usado para intrusión de los datos
5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	La protección de los datos, es una suerte de trabajar en conjunto entre el antivirus, protocolos seguros, perfiles. Hay una técnica llamada NEED TO KNOW que significa tener acceso a aquello que requiera saber para el correcto funcionamiento de sus funciones. Es importe	• Trabajar en conjunto entre el antivirus, protocolos seguros y perfiles. • Aplicar NEED TO KNOW • Certificaciones de perfiles • Revisiones de LOGS

		realizar certificaciones de los perfiles de los usuarios, estas revisiones deberían realizarse con alguna periodicidad para reducir fuga de información, robo de operaciones y operaciones sospechosas. Por otra parte, las revisiones de los LOGS también es parte de la seguridad para verificar que las personas se están autenticando desde sus propios equipos menores para reducir fraudes. Los niveles de acceso también son revisados por los procesos de auditoria y estos deberían ser revisados a través de herramientas para que sean direccionados a las diferentes áreas de las entidades financieras.	• Revisión de niveles de acceso
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	No tener un acuerdo de nivel de servicio llama al desorden ya que afectaría a la disponibilidad, sobre todo dar la tranquilidad a los clientes de acceder a su información, por otra parte a nivel de auditoria los SLA tanto con los proveedores como con las áreas usuarias se usan para verificar si existen brechas. Estos SLA son ajustables de acuerdo a la realidad de cada	• No tener un acuerdo llama al desorden • Mantener un SLA con proveedores y áreas usuarias • Los SLA son ajustables de acuerdo a la realidad de cada organización

		organización o de lo que requiere el usuario para atender sus operaciones. Es importante revisar los acuerdos respecto a los BECHMARKING que ya están estipulados en el sector o seguir las buenas prácticas. El análisis de impacto es importante para determinar los procesos críticos para activar los servicios más prioritarios debido a que no todo se podrá levantar a la vez, esto tiene que estar alineado con las áreas usuarias para verificar si es factible activarlo en un determinado tiempo o en su defecto verificar si la infraestructura actual la soporta caso contrario se requería realizar inversiones. El BIA debe ser escalado y aprobado al más alto nivel. El BIA se debe de realizar de manera anual y es responsabilidad del área usuaria.	• Revisar los BECHMARKING • El análisis de impacto es importante para determinar procesos críticos • El BIA debe ser escalado y aprobado al más alto nivel

N°	**Preguntas**	**Entrevistado 3 -** Information Policy and Planning Consultant	**Entrevista 3 Codificada**
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	Las tarjetas de crédito se deben de rediseñar ya que el problema sigue siendo la autenticación. La gran diferencia entre los estados unidos y Perú es el nivel cultural en la administración de la tarjeta de crédito ya que la confianza es uno sus los pilares principales.	• Las tarjetas de crédito se deben rediseñar • Cultura en la administración de la tarjeta de crédito
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	Inicialmente todas las empresas que procesaban las tarjetas de pago manejaban sus propios estándares tales como VISA, MASTERCARD, por otro lado, además la familia PCI-DSS también se encuentra PCI-CP (Card Production) quienes se encargan de la construcción de las tarjetas de crédito, adecuación del CHIP, etcétera. Por otro parte, también existen estándares para aplicaciones que sirven para realizar pagos entre las entidades financieras.	• PCI-DSS (Payment Card Industry Data Security Standard • PCI-CP (Payment Card Industry Card Production)
3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	Siempre se debe de contar con un firewall tanto fuera como dentro del perímetro y segmentar la red de tal manera de proteger todos los equipos	• Firewall tanto fuera como dentro del perímetro • Protección malware

		que si son PCI, es importante que los servicios estén disponibles pero cara a la seguridad no guarda relación con la confidencialidad o integridad de las tarjetas de pago ya que no hay compromisos de datos, por otra parte, si los dispositivos electrónicos no están disponibles un atacante puede aprovechar en introducir un malware ya que podría no tener los mismos mecanismos de seguridad como en producción en caso de estar trabajando en DRP.	• DRP (Disaster Recovery Planning)
4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	La protección de las tarjetas de pagos se basa en mantener la confiabilidad de los datos desde que se crea hasta que se utiliza, es el ciclo de vida de las tarjetas de pago. Sino aseguras confiabilidad significa que los datos no están protegidos. Para la transmisión de datos es importante cifrar como por ejemplo usando el protocolo TLS y también los datos que están en reposo. La restricción del acceso físico reduce la fuga de la información y es una de las capas de seguridad.	• Implementar un ciclo de vida de las tarjetas de pago • Cifrar • Protocolo TLS • Restricción del acceso físico

5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	Para que alguien cambie los datos es porque hay una intencionalidad o sea manipulado sea interna o externa. La función del antimalware es detectar programas maliciosos ya sea instalado en las PC o servidores, aunque el reto de los fabricantes es detectar el día cero y que sean configuradas con solo las listas blancas.	• Antimalware • Detectar día cero • Listas blancas
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	Los acuerdos de nivel de servicio están orientado a los controles, no está directamente relacionado a la protección de datos de las tarjetas de pago a nivel de confiabilidad o integridad sin embargo es importante definir bien los indicadores y métricas. Se deben de contar con las herramientas necesarias para monitorear diferentes tipos de ataque.	• Orientado a controles • No está relacionado a la protección de los datos de las tarjetas de pago • Definir indicadores y métricas • Monitorear diferentes tipos de ataques

Anexo 5:

Matriz de entrevistados y conclusiones

N°	Preguntas	**E1-** Consultor Senior Internacional en seguridad de la información	**E2-** Auditor Senior en seguridad de la información	**E3-** Information Policy and Planning Consultant	Similitud	Diferencia	Conclusión
1	¿Qué estrategias se debería tener para mejorar la protección de las tarjetas de pago?	• Identificar todos los dispositivos electrónicos • Determinar los equipos que procesen, trasmitan y almacenen información • Depurar los dispositivos electrónicos innecesarios • Implementar controles	• Hacer revisión cruzada entre las transacciones financieras y contables • Machine Learning ayudará a identificar patrones • Controles para enviar alertas en caso de un evento • Los validadores son importantes para determinar el tipo de consumo	• Las tarjetas de crédito se deben rediseñar • Cultura en la administración de la tarjeta de crédito		E1, E2, E3	• Aplicar las configuraciones técnicas a aquellos equipos que comprometan la seguridad del negocio. • Revisar las transacciones financieras que escapen de los patrones de comportamiento habituales. • Capacitar al usuario final en el manejo de las tarjetas de pago Categorías y subcategoría emergente

							• La revisión cruzada es una categoría • La cultura es una subcategoría
2	¿Cuáles son los estándares de seguridad aplicables a las tarjetas de pago bancarias?	• PCI-DSS • P2P (Peer to Peer) • PIN Security • APS (Application Package Standard) • Seguridad software • Seguridad física • Estándar de pagos sin contacto	• PCI-DSS • ISO 27001 • COBIT	• PCI-DSS (Payment Card Industry Data Security Standard • PCI-CP (Payment Card Industry Card Production)	E1=E2=E3		• Determinar el estándar de seguridad más adecuado para las tarjetas de pago • El estándar de seguridad no es solo para el acceso sino también para la construcción de la misma. Categorías y subcategoría emergentes • La ISO 27001, es una subcategoría • PCI-CP, es una subcategoría
3	¿Qué recursos tecnológicos permite a la disponibilidad, de mayor seguridad en las tarjetas de pago?	• Inventarios actualizados • Actualizaciones de parches • Control de cambios	• Es más importante la confidencialidad e integridad • Las transacciones financieras se deben	• Firewall tanto fuera como dentro del perímetro	E1=E3	E2	• Los equipos de seguridad perimetral permiten el acceso y no acceso a los datos

		• Firewall • Activación de LOGs • Contraseñas de más de 20 caracteres • Planes de DRP	de ejecutar en cualquier momento	• Protección malware • DRP (Disaster Recovery Planning)			• La implementación de un DRP permite la continuidad del negocio.
4	¿De qué manera la confidencialidad permite la protección de los datos de las tarjetas de pago?	• Cifrar para proteger los datos • Mínimo privilegio a través de perfiles • Implementar listas blancas • Controles físicos • Bitácoras • Cámaras de seguridad • Análisis de vulnerabilidad • Capacitación de técnicas de código seguro • Revisión de los programas por expertos	• La restricción física no asegura la protección de los datos • El cifrado protege la información • Todos los colaboradores de la organización deben de estar alineados • El factor humano es el más sensible en toda la cadena de la seguridad • Ingeniería social es el más usado para intrusión de los datos	• Implementar un ciclo de vida de las tarjetas de pago • Cifrar • Protocolo TLS • Restricción del acceso físico	E1=E3	E2	• El cifrado de los datos permite la confidencialidad de la información • Los colaboradores deben estar siempre entrenados para tomar una acción ante un posible evento de seguridad • Las organizaciones deben de crear políticas claras para su aplicabilidad tecnológica. Categorías y subcategoría emergentes • Las Listas blancas, es una subcategoría

							• El factor humano, es una categoría
5	¿Cómo reducir el riesgo de alteración para mantener la integridad de los datos?	• Implementar la tecnología MFA (Multi Factor Authentication) • Instalación de IDS/IPS • FIM (File Integrity Monitoring)	• Trabajar en conjunto entre el antivirus, protocolos seguros y perfiles. • Aplicar NEED TO KNOW • Certificaciones de perfiles • Revisiones de LOGS • Revisión de niveles de acceso	• Antimalware • Detectar día cero • Listas blancas		E1, E2, E3	• La doble autenticación a través del MFA permitirá reducir el riesgo de la intrusión no deseada. • La aplicación de listas blancas sobre los perfiles de usuarios mitiga la alteración de los datos no previstos. Categorías y subcategoría emergentes • Need to Kown, es una subcategoría • FIM, es una subcategoría
6	¿Es importante contar con un acuerdo de nivel de servicio para los dispositivos electrónicos que dan soporte a las tarjetas de pago?	• No está relacionado con la protección de las tarjetas de pago • Enfocado en encontrar la causa del incidente • Análisis forense.	• No tener un acuerdo llama al desorden • Mantener un SLA con proveedores y áreas usuarias • Los SLA son ajustables de acuerdo a la	• Orientado a controles • No está relacionado a la protección de los datos de las tarjetas de pago	E1=E3	E2	• Se debe de definir un BIA de acuerdo al criticidad del servicio • Se debe de definir indicadores para monitorear el servicio con el proveedor

			realidad de cada organización • Revisar los BECHMARKING • El análisis de impacto es importante para determinar procesos críticos • El BIA debe ser escalado y aprobado al más alto nivel	• Definir indicadores y métricas • Monitorear diferentes tipos de ataques			• Los indicadores son ajustables en el tiempo

Conclusión de las entrevistas semiestructura:

Se concluye, que para la protección de los datos de las tarjetas de pago se debe de tener en cuenta tres pilares de seguridad, los cuales son, la disponibilidad, la confidencialidad e integridad de los datos, por otra parte, la arquitectura tecnológica juega un papel crucial debido a que se debe de tener en cuenta las características de los dispositivos electrónicos, sus configuraciones y la administración para el correcto funcionamientos de los servicios. Adicionalmente es fundamental contar con los lineamientos de seguridad claros para definir el tratamiento de la información, como es el caso de cifrar los datos y restringir los accesos para reducir ataques de denegación de servicio, fuga de información que signifiquen accesos no autorizados. Finalmente, las políticas de seguridad tienen que ir acompañado de una cultura de seguridad organizacional para tomar conciencia de las implicancias que estás puede ocasionar si es que no se toma en consideración.

Anexo 6:

Guía de observación

Ubicación:	Cercado de lima
Área:	Tecnología
Observador:	Carlos Javier Montalvo Vivar

Redacción de lo observado sobre tres personas que trabajan dentro de la unidad de estudio, donde P1: Jefe de infraestructura, P2: Jefe de seguridad operativa y P3: Especialista en canales electrónicos.

P1: Es quien tiene a su cargo las áreas de comunicaciones de datos, servidores, base de datos, aplicaciones MIDDLE WARE, aplicaciones CORE y a la vez se encarga de coordinar con los distintos operadores de comunicaciones y centros de procesamiento para el correcto funcionamiento de los servicios financieros para nuestros clientes además es quien acompaña al cumpliendo las normas regularizadas por la súper intendencia de banca y seguros y el Banco central de reserva del Perú, en esa misma línea, una de las principales funciones es analizar y evaluar la viabilidad de los recursos tecnológicos y de seguridad para la implementación de los canales electrónicos que usan las tarjetas pago como medio para realizar transacciones financieras. Para reducir el riesgo de intrusión, el Jefe de infraestructura se encarga de consolidar, holísticamente con los operadores locales e internos los mecanismos tecnológicos y procesos más adecuados para que el uso de las tarjetas de pago cumpla con el estándar de la industria local y que a través de las certificaciones de seguridad como el Ethical Hacking y auditorias se pueda validar de forma periódica con la finalidad de documentar GAPs de seguridad y se puedan levantar las observaciones. De acuerdo al Jefe de Infraestructura una de las mejoras que se puede implementar en la tarjeta de pago es el envío informativo de mensajes de las transacciones realizadas , cambiar de banda magnética a CHIP y que permita la desactivación de operaciones por internet a través de la banca móvil, por otra parte, la propuesta tecnológica de cambiar el uso del PIN en los ATM por el uso de sistemas biométricos a través del reconocimiento facial y en vez de utilizar el código CVV para las compras por internet usar un doble factor de autenticación

mediante códigos SMS y mecanismos de geolocalización, a su parecer reduciría el fraude cibernético e incluso el robo físico por disposición de efectivo en ATM.

P2: Es el que tiene a cargo la ejecución de los lineamientos de seguridad, la creación y asignación de los perfiles de todas las aplicaciones, la custodia de las claves, la elaboración de normas y procedimientos y la gestión de proyectos, por otra parte, asegurarse de cumplir las resoluciones a nivel de seguridad de la súper intendencia de banca y seguros además de participar en los exámenes de auditoria tanto locales como internacionales a fin de cubrir los estándares de seguridad exigidos por el negocio. De acuerdo al Jefe de seguridad operativa, una de las mejoras que se pueden implementar a la tarjeta de pago es permitir el bloqueo de la tarjeta a través de la banca móvil. Con respecto a la propuesta de implementar un sistema biométrico en los ATM si lo considera factible y apropiado, en lo que respecta a la aplicabilidad del doble factor de autenticación mediantes código de mensajes de texto y la técnica de geolocalización lo ve poco flexible sin embargo incrementa la seguridad en gran medida con la finalidad de reducir el robo de dinero de las cuentas bancarias.

P3: Es quien se encarga de administrar y configurar los servidores, adicionalmente analizar las vulnerabilidades por tipo de sistema operativo y versión de las herramientas del negocio, también vela por ejecutar las buenas prácticas de los exámenes de auditoria y Ethical Hacking, mantener una relación constante con el área de seguridad de la información con el fin de seguir los lineamientos y estándares actuales de seguridad, finalmente de diseñar la operatividad de los diversos canales electrónicos que están relacionados con la transacciones financieras a través de la nube y con los planes de recuperación de desastre en caso de una indisponibilidad de los servicios principales. Por otra parte, el especialista de canales electrónicos considera fundamental que para mejorar la seguridad de las tarjetas de pago es reforzar la actualización del criptograma EMV en base a una periodicidad y encaminar el cambio de banda magnética por CHIP para proteger los datos de los clientes y mejorar su confiabilidad con el fin de reducir los fraudes electrónicos. Por otro lado, la propuesta de implementar un sistema de reconocimiento facial en todos los ATM considera que sería clave para reducir los robos de dinero en los cajeros electrónicos ya que necesariamente el agraviado tendría que estar físicamente

frente al dispensador sin embargo, también considera que se tendría que cambiar la arquitectura de los ATM tanto a nivel de hardware y de software, adicionalmente la propuesta de cambiar el CVV por un mecanismo de seguridad de doble autenticación a través de códigos de mensaje de texto y de geolocalización considera que sería indispensable implementarlo para reducir en gran medida las compras fraudulentas realizadas tanto por internet o un establecimiento físico comercial.

Conclusión de la guía de observación

Siendo mi unidad análisis el área de tecnología y en base a las tres observaciones, concluyó que para la protección de los datos de las tarjetas de pago se tiene que diseñar una arquitectura tecnológica que permita cubrir los tres pilares de seguridad como son la disponibilidad, confidencialidad e integridad de los datos, por otra parte, observo que cuentan con los mecanismos de seguridad a nivel de infraestructura y procedimientos que permiten el aseguramiento de los datos sin embargo, si es necesario realizar algunas mejoras a nivel funcional y técnico, como por ejemplo, bloquear la tarjeta de pago, desactivar funciones de compras por internet desde la aplicación móvil y finalmente, coordinar con las entidades a fines para la masificación del lector por CHIP en vez de banda magnética para aumentar la seguridad de las operaciones financieras.

Anexo 7

Ficha de análisis documental

Ubicación :	Cercado de lima
Área :	Tecnología
Observador :	Carlos Javier Montalvo Vivar

Título de la publicación: Resolución SBS 504-2021

Autor(es) : La superintendencia de banca y seguros y administradora privada de fondos y pensiones

Número de la publicación: 504-2021

Fecha de publicación: 19 de febrero del 2021

Tipo de documento: Norma

Lengua: Peruana

Página inicial: 1

Página final: 23

Resumen: Esta resolución está compuesta por cuatro principales aspectos para la protección de la información.

1. Sistema de gestión de seguridad de la información y ciberseguridad
   Es el conjunto de políticas, procesos, procedimientos, roles y responsabilidades que tiene por objetivo asegurar la disponibilidad, la confidencialidad y la integridad de la información.
2. Comité de riesgos
   Dentro de sus principales objetivos son la aprobación del sistema de seguridad de la información y ciberseguridad, fomentar el plan de capacitación a los colaboradores de la organización, finalmente fomentar la cultura de riesgos.
3. Medidas mínimas de seguridad de la información
   - Seguridad de los recursos humanos
   - Controles de acceso físico y lógico
   - Seguridad en las operaciones
   - Seguridad en las comunicaciones
   - Adquisición, desarrollo y mantenimientos de sistemas
   - Gestión de incidentes de ciberseguridad

- Seguridad física y ambiental
- Criptografía
- Gestión de activos de información

4. Aplicación de la ciberseguridad

   Su aplicación está orientado para aquellas empresas del sector financiero que tienen sus aplicaciones en el ciberespacio, los cuales deben de contar con ciertos lineamientos tal como se indica

   - Identificación de los activos de la información
   - Protección frente a amenazas
   - Detección de incidentes
   - Respuestas de respondan sobre el impacto de incidentes
   - Recuperación de los servicios

Descriptores: Resolución de sistema de información

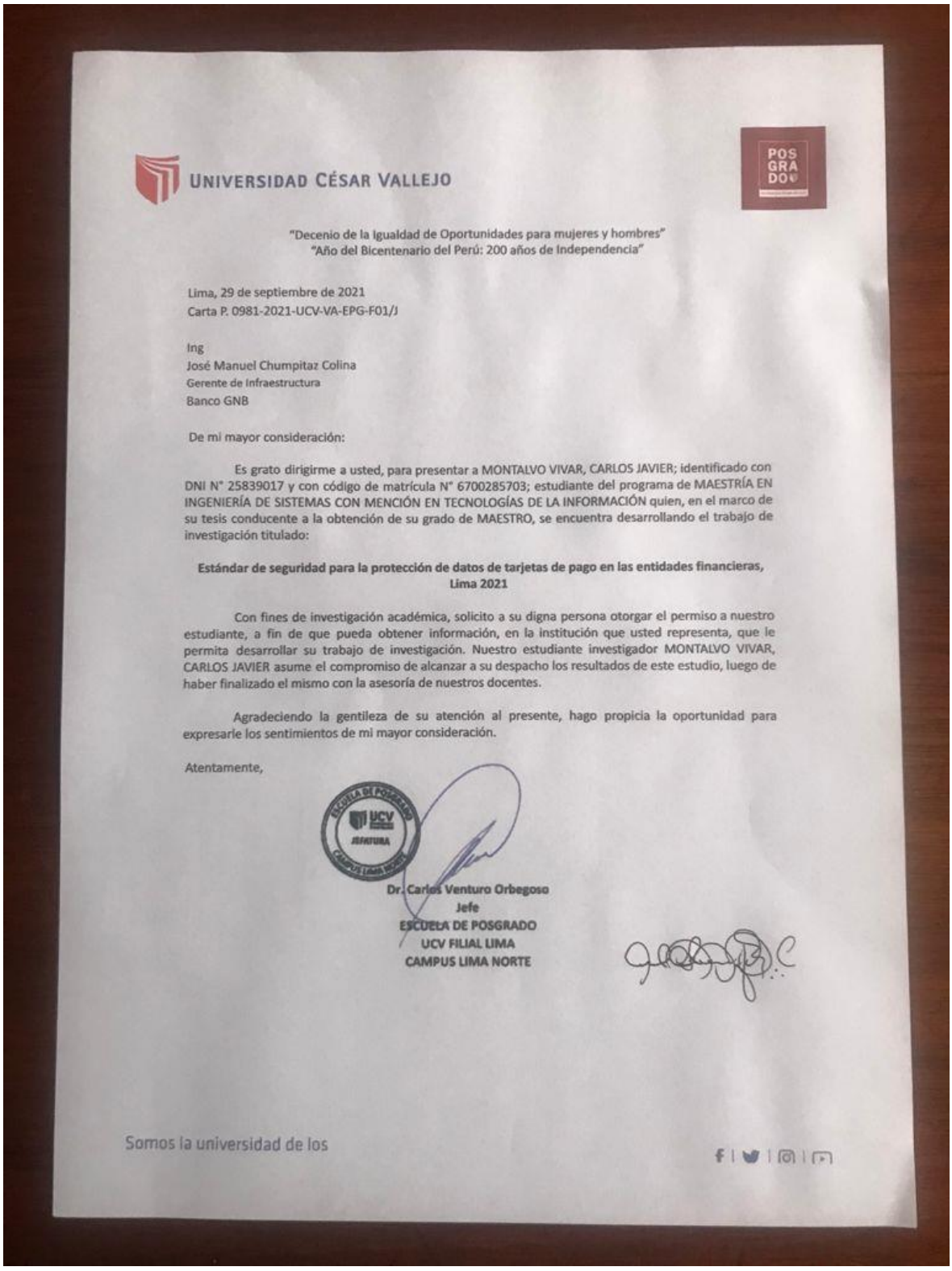
Clasificación: Seguridad

Conclusión del análisis documental:

Después de analizar la norma de la superintendencia de banca y seguros, concluyo que los mecanismos de seguridad que se deben de implementar deben de estar enfocados en la protección de datos de las tarjetas de pagos tanto dentro como fuera de la organización de la red y que estás medidas deben de estar normadas en una política de seguridad para su aplicación, actualización y monitoreo. Adicionalmente, contar con un plan de capacitación que permita informar a los colaboradores de los riesgos y fraudes que podrían estar expuestos en caso de no seguir los lineamientos de seguridad. Finalmente, en caso de materializarse el evento, la entidad financiera deberá activar sus protocolos de contingencia para dar continuidad a los servicios.

Anexo 8:

Carta de autorización de investigación de tesis



UNIVERSIDAD CÉSAR VALLEJO

POSGRADO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

Lima, 29 de septiembre de 2021
Carta P. 0981-2021-UCV-VA-EPG-F01/J

Ing
José Manuel Chumpitaz Colina
Gerente de Infraestructura
Banco GNB

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a MONTALVO VIVAR, CARLOS JAVIER; identificado con DNI N° 25839017 y con código de matrícula N° 6700285703; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador MONTALVO VIVAR, CARLOS JAVIER asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dr. Carlos Venturo Orbegoso
Jefe
ESCUELA DE POSGRADO
UCV FILIAL LIMA
CAMPUS LIMA NORTE

Somos la universidad de los

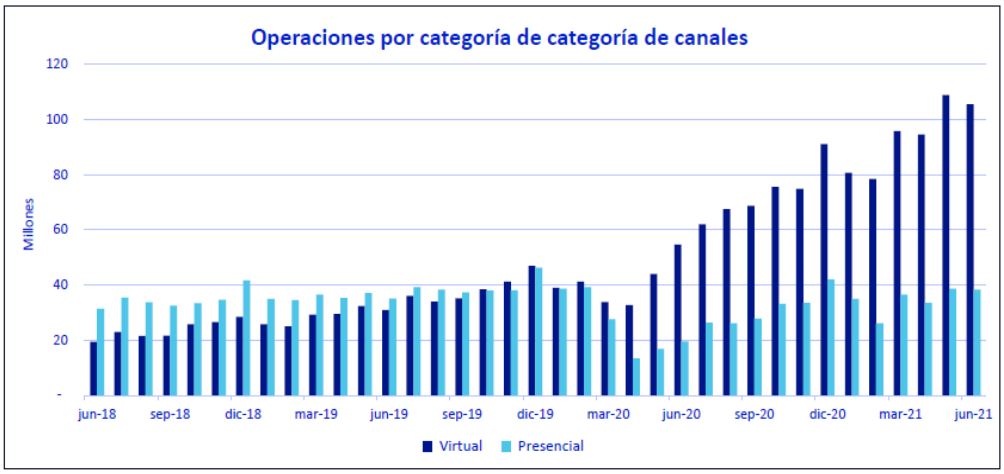
Anexo 9:

Estadísticas de medios de pago e incidentes

Tal como se muestra figura 3 el incremento de los canales virtuales aumento del 37% al 71% y una tendencia a la baja del medio de pago presencial del 60% al 26%. Por otro lado, este aumento en el uso de los canales virtuales ha desencadenado un incremento de incidentes en su mayoría relacionados a fraudes cibernéticos en el uso de los canales electrónicos del 36% al 75%, tal como se muestra en la figura 4

Figura 3

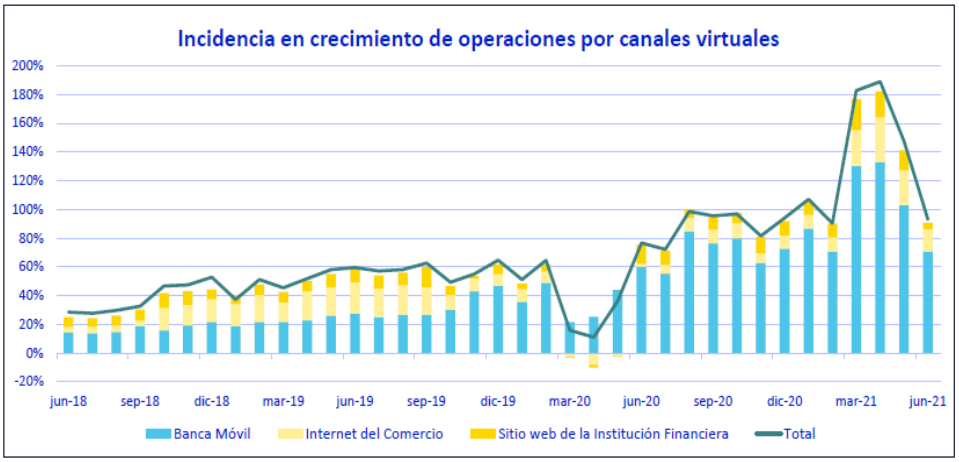
Medios de pago más utilizados



Fuente: ASBANC

Figura 4

Incidentes en los canales virtuales



Fuente: ASBANC

Anexo 10:

PROPUESTA

Portada

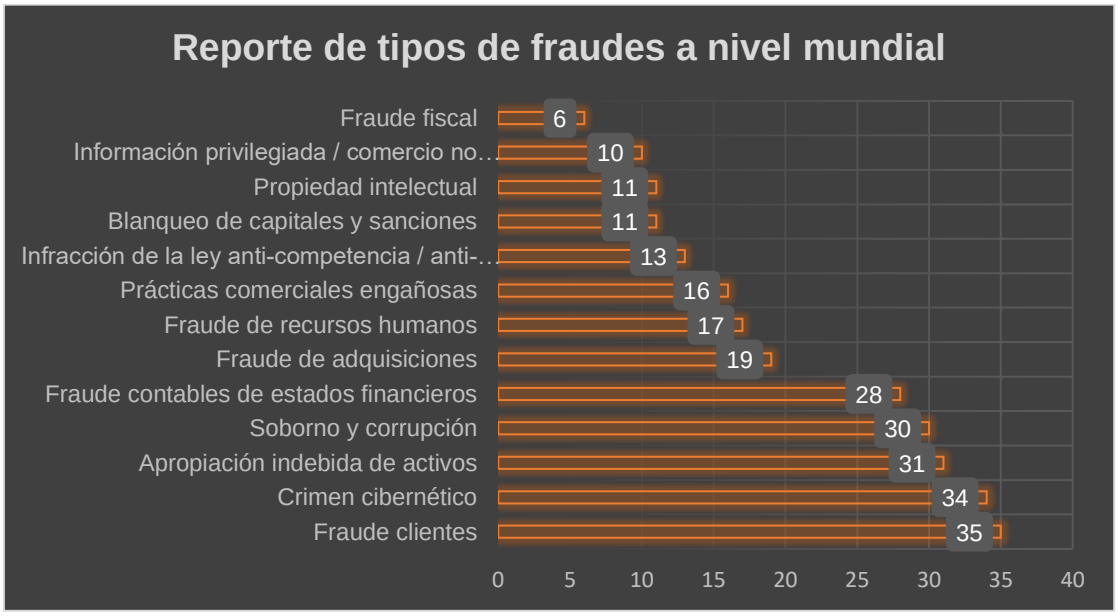
Investigador:	*Carlos Javier Montalvo Vivar*
Título de la investigación:	Estándares de seguridad para la protección de datos de las tarjetas de pago

Formulación del problema

La implementación de estándares de seguridad permitirá reducir el riesgo de la materialización de ataques cibernéticos que generen indisponibilidad de los dispositivos electrónicos, alteraciones de los datos de los clientes y acceso a los datos de personas no autorizadas. Por otro parte, si es que no se aplica una arquitectura tecnológica de última generación, los clientes podrían estar expuestos a fraudes y/o robo de sus cuentas bancarias. Según la encuesta global sobre fraudes y delitos económicos de PwC (2020) el costo total de pérdidas por estos tipos de crímenes fue de 42,000 billones de dólares en tan solo dos años y en Perú fue de 4,782 millones de dólares, tal como se muestra en la figura 10.

Figura 10

Tipos de fraudes a nivel global por impacto económico



Fuente: PwC Global Economic Crime and Fraud Survey

Hoy en día muchos de los estándares de seguridad que se vienen implementado en distintas organizaciones financieras no cumplen con el objetivo de proteger los datos de las tarjetas de pago, la lista se encuentra en la tabla 8

Tabla 8

Listado de estándares tradicionales

Estándares	Descripción
PCI-DSS	Payment Card Industry Data Security Standard, permite proteger la información sensible de las tarjetas de pago
PCI-CP	Payment Card Industry Card Production, definen los criterios de seguridad física y lógica que deben ser implementados durante los procesos de producción y el suministro de tarjetas de pago.
ISO 27001	Encargada de emitir los lineamientos de seguridad en la organización.

Solución estimada:

Si bien es cierto que los estándares tradicionales son también elementos importantes para mitigar los riesgos de disponibilidad, integridad y confidenciales no son suficientes para reducir el índice de robo y/ fraude cibernético ya sea por un canal virtual (Banca móvil / Banca por internet) o un medio físico (ATM / Puntos de venta). En la tabla 9 se indica los estándares de seguridad emergentes que si permiten en mayor porcentaje solucionar toda clase de crimen informático.

Para el caso de disposición de efectivo tanto en los ATM como en los puntos de ventas de los comercios se propone el uso del MFA es decir seguir colocando el PIN de 4 dígitos y adicionalmente la implementación de un sistema de biométrico con la finalidad de asegurar que la persona que desea realizar la transacción se identificada. Por otra parte, para el caso de los canales virtuales, la propuesta es utilizar el MFA, la primera validación sería el envío de un mensaje de texto con un código de verificación al número celular previamente registrado, la segunda verificación sería la geolocalización a través del GPS y triangular la ubicación del teléfono y la tarjeta de pago, adicionalmente la autenticación de un sistema de biometría, finalmente un sistema Machine Learning para que en caso de detectar un comportamiento inusual en la cuenta se pueda bloquear de forma automática. En la tabla 9 se indican los nuevos estándares

Tabla 9

Listado de estándares emergentes

Estándares	Descripción
Biometría	Reconocimiento de huella dactilar, facial y de retina
Machine Learning	Sistemas informáticos que permiten el autoaprendizaje de patrones de comportamientos
Autenticación por doble factor de autenticación (2FA)	Este estándar permite tener acceso a la información a través de una doble autenticación usando un código SMS, una llamada telefónica o de una llave aleatoria.
Geolocalización	Es un estándar que permite triangular entre el teléfono móvil y la tarjeta de pago con su ubicación para realizar la transacción.