FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

“PROPUESTA DE HERRAMIENTA INTEGRADORA DE ANÁLISIS Y PREVENCIÓN DE FRAUDE PARA BANCO DAVIVIENDA HONDURAS”

SUSTENTADO POR:

MARÍA FERNANDA RODRÍGUEZ RIVERA

RAMÓN ALBERTO RIVERA VILLATORO

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN DIRECCIÓN EMPRESARIAL

TEGUCIGALPA, M.D.C. F.M. HONDURAS, C.A.

FEBRERO 2022

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON ANTONIO BREVÉ REYES

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DIRECTORA NACIONAL DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

“PROPUESTA DE HERRAMIENTA INTEGRADORA DE ANÁLISIS Y PREVENCIÓN DE FRAUDE PARA BANCO DAVIVIENDA HONDURAS”

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

ASESOR METODOLÓGICO

VIANNEY PATRICIA VILLALTA RIVERA

ASESOR TEMÁTICO

IDALIA CAROLINA CÁRCAMO

MIEMBROS DE LA TERNA:

ALBERTINA NAVARRO-RÍOS

MARCELO FLORES

MARLON MEJÍA

DERECHOS DE AUTOR

María Fernanda Rodríguez Rivera

Ramón Alberto Rivera Villatoro

AUTORIZACIÓN DEL AUTOR(ES) PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN

ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS DE POSTGRADO

Señores

CENTRO DE RECURSOS PARA

EL APRENDIZAJE Y LA INVESTIGACIÓN (CRAI)

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA (UNITEC)

Tegucigalpa

Estimados Señores:

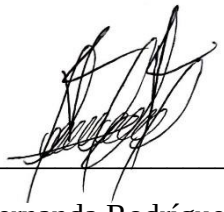
Nosotros, María Fernanda Rodríguez Rivera y Ramón Alberto Rivera Villatoro, de Tegucigalpa, autores del trabajo de postgrado titulado: Propuesta de una herramienta integradora de análisis y prevención de fraudes para Banco Davivienda, presentado y aprobado en el mes de enero 2022, como requisito previo para optar al título de máster en Dirección Empresarial y reconociendo que la presentación del presente documento forma parte de los requerimientos establecidos del programa de maestrías de la Universidad Tecnológica Centroamericana (UNITEC), por este medio autorizo a las Bibliotecas de los Centros de Recursos para el Aprendizaje y la Investigación (CRAI) de UNITEC, para que con fines académicos puedan libremente registrar, copiar o utilizar la información contenida en él, con fines educativos, investigativos o sociales de la siguiente manera:

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

De conformidad con lo establecido en los artículos 9.2, 18, 19, 35 y 62 de la Ley de Derechos de Autor y de los Derechos Conexos; los derechos morales pertenecen al autor y son personalísimos, irrenunciables, imprescriptibles e inalienables. Asimismo, el autor cede de forma ilimitada y exclusiva a UNITEC la titularidad de los derechos patrimoniales. Es

entendido que cualquier copia o reproducción del presente documento con fines de lucro no está permitida sin previa autorización por escrito de parte de UNITEC.

En fe de lo cual se suscribe el presente documento en la ciudad de Tegucigalpa, a los 15 días del mes de diciembre del año 2021



María Fernanda Rodríguez Rivera

12013021

Ramón Alberto Rivera Villatoro

12013302

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

FACULTAD DE POSTGRADO

"PROPUESTA DE HERRAMIENTA INTEGRADORA DE ANÁLISIS Y PREVENCIÓN DE FRAUDE PARA BANCO DAVIVIENDA HONDURAS"

María Fernanda Rodríguez Rivera

Ramón Alberto Rivera Villatoro

Resumen

La presente investigación tiene como objetivo, proponer una herramienta integradora de análisis y prevención de fraude, que se hará a través de la indagación de componentes esenciales en el proceso como ser: la experiencia de expertos en el tema, regulaciones y leyes que intervienen en el mismo y demás. Se inicia analizando aspectos teóricos y conceptos relevantes en el tema como ser: tecnología, comercio electrónico, para luego describir la metodología usaba que se basó en la aplicación de entrevistas a personas involucradas en el tema y un proceso de observación en la ejecución del proceso de análisis por los analistas encargados. Seguidamente, se analizaron los resultados de la misma, llevando a las conclusiones y recomendaciones en las que se fundamentó la propuesta a Banco Davivienda, logrando disminuir tiempos de ejecución que apoyará a eficientizar el proceso de análisis y por consiguiente, asegurar la confiabilidad del cliente y la satisfacción del mismo.

Palabras clave: Comercio electrónico, experiencia de especialistas, fraude electrónico, tecnología.

GRADUATE SCHOOL

"PROPOSAL FOR AN INTEGRATIVE FRAUD ANALYSIS AND PREVENTION TOOL FOR BANCO DAVIVIENDA HONDURAS"

María Fernanda Rodríguez Rivera

Ramón Alberto Rivera Villatoro

Abstract

The objective of this research is to suggest a centralize fraud analysis and prevention tool, which will be executed through the investigation of essential components in the process such as: the subject matter expert's experience, regulations and laws that intervene the process itself. The process begins by analyzing theoretical aspects and relevant concepts on the subject such as: technology, electronic commerce. The approach used was based observations to the analytic procedure done by the Analyst and on interviews with people involved in the subject. Subsequently, the results were analyzed, leading to the conclusions and recommendations on which the proposal to Banco Davivienda was based, managing to reduce performance times that will help to make the analysis process more efficient and, therefore, ensure the reliability of the client and its satisfaction.

Keywords: e-commerce, electronic fraud, specialist experience, technology.

DEDICATORIA

A mi hijo Henry David Rodríguez Rivera por ser mi inspiración siempre y ser mi fuente de paz y tranquilidad en los momentos que más he necesitado.

A mis padres Marlen Rivera y José Francisco Rodríguez por no soltar mi mano en ningún momento y ser mi apoyo incondicional en cada proceso de mi vida, para ellos son todos mis logros.

A mi hermano Francisco Rodríguez que sin duda ha sido mi mejor amigo y fiel acompañante en las noches de desvelo, por hacerme ver cosas que, en medio de tanto estrés y trabajo, yo no veía con claridad.

María Fernanda Rodríguez Rivera.

A mi madre Rosa Villatoro que sin duda con su ejemplo ha sido mi basto y motivación para seguir sobre este objetivo personal y sin olvidar en este camino los valores que me inculcó.

Y a mis hermanos carnales e espirituales, compañeros de trabajo y amigos por ser parte de cada uno de los acontecimientos que a lo largo de esta preparación me apoyaron.

Ramón Alberto Rivera Villatoro.

AGRADECIMIENTO

A DIOS todo poderoso por darnos el entendimiento, discernimiento, por guiar nuestro camino de manera positiva hacia la culminación de nuestros estudios universitarios, por darnos la fuerza y sabiduría en cada etapa de nuestras vidas, por brindarnos salud, disciplina, perseverancia e inteligencia en el cumplimiento de este objetivo profesional.

A LA UNIVERSIDAD TECNOLOGICA CENTROAMERICANA (UNITEC), y a su grupo de catedráticos que con empeño y servicio nos trasmitieron conocimiento y motivaron al desarrollo de nuestras habilidades, las cuales serán necesarias para nuestro desenvolvimiento profesional al que ahora nos enfrentaremos.

A la MASTER PATRICIA VILLALTA, asesora de la tesis, por su tiempo, paciencia, amabilidad, consejos y asesoramiento, lo que nos ayudó a concluir nuestra tesis con éxito.

A BANCO DAVIVIENDA, por brindarnos su tiempo, su esfuerzo, e información deseada para realizar nuestra tesis.

A LOS MIEMBROS TERNA DE LA TESIS, por su valiosa asesoría y juicio profesional.

EN GENERAL a cada una de las personas que de una u otra forma colaboraron para obtener nuestro título universitario.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPITULO I. PLANTEAMIENTO DEL PROBLEMA

1.1.Introducción

Los servicios financieros ofrecidos a la población han variado a través de los años y con esto, la diversidad en ellos, ya sean préstamos, cuentas de ahorro, tarjetas de débito y crédito, entre otros. De igual forma, en la medida que el número de usuarios, y la diversidad de servicios que éstos consumen crece, los riesgos y ataques de organizaciones delictivas ya sean digitales o presenciales aumenta al mismo tiempo.

Durante la pandemia COVID-19, esta problemática ha tenido un aumento ya que la mayoría de las personas han adaptado sus transaccionalidades a modo digital, así como los comercios y negocios sumaron a sus ofertas la opción de compras en línea. Estos cambios surgidos, alimentan la cobertura de dichas organizaciones delictivas ya que la población meta aumenta y con ella la vulnerabilidad, por falta de conocimientos con relación al uso de sus servicios financieros digitales.

Las instituciones financieras trabajan día a día para combatir o disminuir estos ataques constantes a la seguridad financiera de sus usuarios, sin embargo, en el proceso se destacan ciertas brechas que no son cubiertas en su totalidad, por lo tanto, se reflejan oportunidades de mejora en el proceso, con el fin de brindar esa seguridad al usuario garantizando así la satisfacción del cliente.

La presente investigación busca indagar en el proceso actual de análisis y prevención de fraudes de Banco Davivienda Honduras, con el fin de detectar estas brechas que podrían ser cubiertas al integrarse la información necesaria en una misma herramienta. El documento consta de 6 capítulos que se distribuyen de la siguiente manera:

En el Capítulo I, se detalla el planteamiento del problema de la investigación realizada en Banco Davivienda Honduras, tales como, antecedentes del problema, objetivos de investigación, definición de variables y la justificación del mismo.

En el Capítulo II, se describen los componentes del marco teórico, los cuales son: análisis de la situación actual de Banco Davivienda, se detallan el macroentorno y microentorno que rodea a la institución, de igual forma, se escriben las teorías que sustentan la presente investigación, y la conceptualización de términos claves de la misma.

En el capítulo III, se encuentra la metodología que guió la investigación para lograr generar una propuesta que cumpla con las necesidades del banco, así como también se describen los métodos de recolección de datos que fueron utilizados.

En el capítulo IV, se desglosan los resultados de los métodos antes mencionados, como ser la entrevista a personas conocedoras del tema que compartieron ideas basadas en su experiencia, así como los resultados de la observación al proceso de análisis y prevención de fraude utilizado por Davivienda.

En el capítulo V, se exponen las conclusiones y recomendaciones resultantes de la investigación consideradas por los autores de la misma, con el fin de brindar una propuesta de mejora al Banco Davivienda.

Y para finalizar, en el capítulo VI, se encuentra detallada la propuesta que pretende mejorar el proceso de análisis y prevención de fraude, misma que servirá como guía para Banco Davivienda, si llegasen a considerar la ejecución de la misma.

1.2.Antecedentes del problema

Banco Davivienda es miembro de las instituciones financieras de Honduras, desde mediados del año 2020 este sistema ha presentado incrementos de más del 100% en la pérdidas

económicas comparado a años anteriores, esto producto de los fraudes a los que los clientes son sometidos por las bandas criminales organizadas, éste incremento está vinculado a que los clientes han migrado su transaccionalidad y uso de sus tarjetas de crédito y débito, a través de las plataformas digitales y comercios electrónicos como una necesidad surgida e identificada durante tiempo de la pandemia COVID-19, a mayor transaccionalidad las instituciones financieras presentan mayor riesgos tantos económicos como reputacionales, y específicamente Davivienda ha registrado pérdidas alrededor de L5.5 millones (Davivienda , 2021)

En aras de mitigar los riesgos, el banco ha realizado acciones y estrategias de modo preventivo, como robustecer las políticas de alertamientos, sin embargo, las mismas han generado sobrecargas laborales de las personas vinculadas en la atención de reclamos, prevención y análisis de fraudes, así como inconformidad de los clientes tanto a los afectados, como los que resultan alertados para confirmación, lo que ha llevado en ocasiones a finalizar relaciones de negocio.

Las transaccionalidad de tarjetas de crédito y débito ha aumentado en un 49%, de este aumento el 80%, proviene de comercios electrónicos y en cuanto a canales digitales el flujo de transacciones realizadas por los clientes en la plataforma de aplicación (APP sus siglas en inglés) ha incrementado en un 26%, estos incrementos de transaccionalidad derivan en una mayor cantidad de alertas basados en reglas de prevención, de las cuales para tarjetas de débito y crédito es de un 34%, y un 837%, para el canal digital denominado APP y en cuanto a gestiones, un incremento del 353%, todos estos datos resultan del análisis de métricas entre el año 2020 al 2021. (Davivienda , 2021)

1.3.Definición del problema

1.3.1. Enunciado del problema

Banco Davivienda Honduras, es una institución financiera dedicada al otorgamiento de productos y servicios. Como parte de sus objetivos estratégicos desde el 2019, ha sido la digitalización de sus productos a través de la innovación, la cual se estimó que sería en una forma gradual en un lapso de 5 años considerando la adaptación de los clientes. Sin embargo, al entrar a la pandemia COVID-19 y con esto al confinamiento de las personas, se presentó un aceleramiento a la migración de uso de canales y productos digitales, ya que los clientes demandaron la utilización de APP, banca por internet y comercios electrónicos. Esto conllevó de igual manera, a un incremento sustancial en los fraudes electrónicos a los cuales son sujetos los clientes y las instituciones financieras, mismos que generan insatisfacción de los clientes y sobrecarga laboral del personal de prevención y gestión de fraudes.

1.3.2. Formulación del problema

¿Cómo DAVIVIENDA puede mejorar el proceso de análisis y prevención de fraudes mediante una herramienta integradora, que comprenda la tecnología, los controles y la experiencia de personas involucradas en el proceso y tema?

1.3.3. Preguntas del problema

1. ¿Cuáles son los factores que influyen en el proceso ejecutado por Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios?
2. ¿Cuáles son los requerimientos técnicos, regulatorios y políticas necesarios para establecer un sistema que pueda utilizar Davivienda para la prevención de fraudes en los canales digitales y comercios?
3. ¿Cómo el proceso de gestión de tecnología e innovación puede apoyar en establecer una herramienta integradora que pueda utilizar Davivienda para la prevención de fraudes en los canales digitales y comercios?

4. ¿Cómo plantear el diseño de una propuesta para una herramienta integradora que pueda utilizar Davivienda para la prevención de fraudes en los canales digitales y comercios?

1.4.Objetivos del proyecto

1.4.1. Objetivo general

Proponer los requerimientos necesarios para la selección de una herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras, mediante la indagación de la tecnología, controles y la experiencia de personas involucrados en el proceso y tema, para apoyar en la eficiencia de los controles de riesgos operativos y el servicio al cliente, así como el mantenimiento de una carga laboral óptima.

1.4.2. Objetivos específicos

1. Conocer los factores que influyen en el proceso ejecutado por Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.
2. Determinar los requerimientos regulatorios, políticas y técnicos que debe de contener un sistema de información que Davivienda pueda utilizar para la prevención de fraudes en los canales digitales y comercios.
3. Considerar el proceso de gestión de tecnología e innovación para la propuesta de una herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.
4. Plantear el diseño para una propuesta de herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.

1.5. Justificación

Banco Davivienda Honduras tiene más de 40 años de estar en el sistema financiero, siendo también miembro del Grupo Bolívar con su casa matriz en Colombia, en la actualidad

cuenta con varios sistemas o herramientas que les permite identificar y analizar alertas de monitoreo sobre transacciones fraudulentas.

Por lo que esta investigación es conveniente realizarla, ya que permitirá establecer mejoras que apoyen en agilidad del proceso, la detección de fraudes y en la tomas de decisiones, así como también será una estrategia mitigante a los fraudes que traerá consigo la reducción de pérdidas monetarias y reputacionales.

De acuerdo con las métricas generadas por el área de Operaciones en Tarjetas al cierre del mes de septiembre, se presenta un aumento sustancial de transacciones y alertamientos de más del 50% (Davivienda , 2021). Por lo que no es ajeno para los líderes de Banco Davivienda que existen brechas que aún hay que cerrar, pero también la conciencia de lo vital que sería implementar una herramienta que pudiera contar con sistemas de inteligencia social, incorporación de referencias crediticias y transaccionalidad de los usuarios, permitiendo que el proceso sea más ágil y por ende establecer acciones oportunas en tiempo y forma, de manera de mantener un equilibrio tanto en el riesgo como en la efectividad de contactación.

Las quejas y reclamos son factores que no aportan a la estrategia de servicios del banco, repercutiendo en las encuestas de satisfacción y lealtad de sus clientes (NPS sus siglas en inglés), es por ello que al considerar la investigación lleva a identificar mejoras e ideas que apoyarán a mitigar este tipo de incidentes.

CAPITULO II. MARCO TEÓRICO

2.1.Análisis de la situación actual.

2.1.1. Macroentorno

2.1.1.1.Entorno Economico

La economía mundial es uno de los colaterales más afectado producto de la crisis sanitaria de la pandemia COVID-19, la cual ha dejado fisuras que hoy en día crean incertidumbre a corto, mediano y largo plazo, las que se tendrán que ir abordando en el tiempo, las dimensiones de los efectos son grandes, desde el desabastecimiento de productos, materia prima y el desempleo, que conllevará alianzas entre las grandes potencias económicas con las más afectadas, sin embargo, se estima que el abastecimiento de vacunas es crucial para retomar las actividades que lleven a una recuperación de la economía.

Uno de los primeros efectos para el 2020 fue la reducción de la economía en las grandes potencias tales como: Estados Unidos de América (EE.UU.) y Japón en un 6.1% y para la zona del euro un 9.1% esto a causa de la toma de medidas de prevención y control. Se previó que para el 2021 la economía mundial creciera en un 0.2% y para el 2022, 1.2% en comparación al 2020. (Banco Mundial, 2020).

La necesidad de la continuidad de negocios conllevó al crecimiento de nuevos comercios electrónicos, siendo esta una estrategia crucial para rehabilitar la economía en todos los países, sin embargo, esto llevó a que algún sector mal intencionado iniciara con fraudes, no solo en temas de compras sino también en el uso de productos financieros. Según el Foro Económico Mundial, es probable que los daños causados por el delito cibernético alcancen los 6 billones de dólares a nivel global hasta finales del 2021, lo que equivale al Producto Interno Bruto (PIB) de la tercera economía más grande del mundo. (PayPal, 2021).

La crisis económica que enfrenta Honduras por la corrupción, en donde se suma la pandemia y los huracanes Eta e Iota que acecharon el territorio, conlleva un aumento significativo de la pobreza y la delincuencia; la pobreza se ha identificado como un factor determinante para que las personas, debido a sus necesidades y carencias de empleo, sean un blanco fácil de reclutamientos de bandas organizadas para que les ayuden a cometer actos delictivos a cambio de una remuneración económica.

> El Boletín Económico N° 15 "La pobreza: condición estructural limitante para el desarrollo económico y social del país", indica que la tasa de pobreza de los hogares hondureños medida a través del Método de la Línea de Pobreza mostró un incremento sin precedentes al pasar de 59.3 de los hogares pobres en el 2019 a una estimación aproximada del 70% en el 2020. (Rodriguez, 2021)

Hay retos importantes a los que el país aún está por enfrentar como temas de política y los bajos niveles de educación que la pandemia ha generado, la educación en materia de uso de la tecnología es muy baja, por lo que es fácil para los ciberdelincuentes encontrar a sus víctimas y que están les brinden toda la información que requieren para realizar el ciberdelitos; para contrarrestar estos temas se requieren contar con profesionales capacitados en el área de seguridad informática y de la información, el mercado internacional está apostando a especialistas con altos estándares en todo los ámbitos de la tecnología, pero más enfocado en el tema de esta investigación se acrecentará más la vulnerabilidad porque la especialidades de esto conllevan muchos temas técnicos y analíticos que aún no están al cien por ciento disponibles en las carreras del área de la tecnología que ofertan las universitarias en el país.

2.1.1.2. Entorno Social

La nuevas generaciones van creando y requiriendo nuevos y mejores productos y servicios, que deben ser innovadores, en los últimos años se ha observado el surgimiento de varias plataformas digitales en donde se ofertan, venden y realizan transacciones financieras

ya sea con sus tarjetas de crédito y débito así como sus cuentas bancarias, que facilitan la utilización de sus productos financieros y hacer negocios haciendo más práctica y ágil la vida de los seres humanos, sin embargo hay algunos que pese a esa ventaja que ofrecen sin importar la cultura y su ubicación, han sido renuentes a dichas plataformas.

La humanidad a lo largo de su historia ha sufrido muchos cambios en aspectos culturales, y económicos que han sido transcendentales y no debemos obviar que el surgimiento y crecimiento tecnológico que se ha llevado a cabo en los últimos años, obligando a las empresas e instituciones a una migración digital, sin embargo, el aparecimiento de la pandemia produciendo una emergencia sanitaria detonada por la COVID-19, la población a nivel mundial se vio obligada al confinamiento, obligándose así hacer uso de plataformas digitales que les permitieran acceder a servicios y productos para su subsistencia.

La pandemia conllevó desafíos que van más allá que hacer frente al virus del COVID-19, sino que además a la migración hacia plataformas digitales, creciendo así los riesgos de fraudes tanto para las instituciones financieras como para sus clientes, el crecimiento digital trae consigo el cibercrimen, mismo que no ve distinción de economías , raza o cualquier otro factor descriptivo de la sociedad, ya que los estafadores han visto una excelente oportunidad por la vulnerabilidad de los sistemas de seguridad, colocando sitios web (*websites)* falsos ofreciendo productos y servicios en línea. En esta investigación se tomó como referencia las experiencias de Latinoamérica y el Caribe, debido a temas culturales que se comparten en los países de esa región, pero también a Los Estados Unidos de Norte América (EE.UU.), considerado una potencia económica y en donde existen una fluidez más considerable de negocio entre las naciones de la zona.

2.1.1.3.Entorno Politico

Durante los ultimos 12 años, Honduras ha experimentado crisis sustanciales en el ámbito de la política, lo que conlleva a una disminución de los inversores internacionales en el territorio. En el reciente gobierno, se han implementado las zonas de empleos y desarrollo económico, como parte de una estrategia de atracción a la inversión sin embargo, es una incertidumbre la finalidad de las mismas, ya que los inversionistas estarán a cargo de la política fiscal, seguridad y de resoluciones de conflicto. (FOSDEH, 2021)

Para el año 2022, se tienen muchas perspectivas debido al cambio de autoridades del gobierno entre ellas, el aumento de los problemas políticos por la resistencia de la oposición, aumento en los precios del combustible y canasta básica, y la inestabilidad en las políticas arancelarias, todo esto generando mayor delincuencia e inseguridad en el pais, que para esta investigación es un factor crucial debido que puede conllevar al aumento de fraudes.

2.1.1.4. Entorno Tecnológico

Si bien es cierto, la pandemia COVID-19 ha dejado grandes brechas negativas, también existen otras que son positivas, en el caso de ésta es la transformación digital de todos los sectores para finales del 2020 e inicio del 2021, proyectando que el porcentaje del producto Interno Bruto (PIB) en la tecnología sería del 5% que representa un 10% a nivel mundial, Honduras no es ajeno a estas tendencias y se estima por ello que se presentará crecimiento, ya que durante la pandemia se ha reflejado un interés por la tecnología y sobre todo por la transformación digital, cambios rápidos que también llevan robustecer las infraestructuras. (CNI, 2020)

La adaptación digital más las nuevas formas de trabajar y hacer negocios, conllevan a enfocar esfuerzos en nuevas variables, Latinoamérica y el Caribe (ALC) se han preocupado sobre el tema de ciberseguridad debido a que existe un alto consumo de internet,

lastimosamente, los usuarios no son conscientes de las medidas de seguridad que deben de tener, pocos países de la región cuentan con estrategias nacionales de ciberseguridad, lo que los expone a ciberataques.

> Hasta principios de 2020, solamente 12 países habían aprobado una estrategia nacional de ciberseguridad (un aumento con respecto a los 5 que tenían este tipo de estrategias en 2016), y únicamente 10 países han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad. (BID; OEA, 2020)

Estados Unidos de Norte América (EE.UU.) cuenta con un centro contra delitos cibernéticos conformado por tres unidades, de las cuales ésta investigación considera oportuno mencionar dos de ellas, la Unidad Contra Delitos Cibernéticos, que provee la gestión y supervisión de investigaciones para las agencias relativas al internet, al focalizarse en las organizaciones criminales transnacionales que utilizan funciones o elementos cibernéticos para extender sus actividades criminales; y la segunda, la unidad de informática forense en donde sus agentes son capacitados para realizar exámenes forenses de dispositivos de almacenamiento digital y soportes informáticos, teléfonos celulares/inteligentes, tabletas y cintas de grabación. Utilizan todas las técnicas de recuperación de evidencia digital disponibles para preservar la autenticidad e integridad de un artículo, manteniendo a la vez una cadena de custodia estricta. (ICE, 2021)

A pesar de contar con estas unidades especializadas y acciones mitigantes se registró el récord de 791,790 denuncias y quejas provenientes de delitos cibernéticos en 2020 que equivalen a una pérdida de US$4,200 millones. En donde el aumento en cuanto a cantidades de denuncia es del 69%, y un 20%, en monto al compararlo contra el año 2019. (FBI, 2020)

Al indagar en los métodos que los defraudadores utilizan para concretizar los actos y acciones delictivas, esta investigación observó que tanto en ALC y EE.UU., el modo de operación concuerdan entre los cuales se pueden mencionar:

Tabla 1. Las principales estafas globales de COVID-19 dirigidas a los consumidores.

Clasificaciones	**Porcentaje afectado por el esquema. Entre los blancos del fraude digital de COVID-19**
Phishing (Manipulación víctimas para que revelen información)	27%
Estafas de vendedores externos en sitios web minoristas en línea legítimos	21%
Estafa benéfica y de recaudación de fondos	19%
Estafa por desempleo	18%
Vacunas, curas, pruebas y EPP fraudulentos contra la COVID-19	15%
Seguro falso	15%
Fraude de envío	14%
Robo de identidad	14%
Tarjeta de crédito robada o cargos fraudulentos	13%
Estafa de cheques de estímulo	12%
Alguien que cambie su información personal o de cuenta a través de un centro de llamadas	12%
Cuenta asumida	11%

Fuente: (TransUnion, 2020)

De igual forma existen factores como la falsificación de documentos de identidad que facilitan aún más las practica de los defraudadores, a continuación, las estafas más significativas por país.

Tabla 2. Estafas en línea de COVID-19 dirigidas a sus consumidores por país.

País	**Tipo de fraude superior**	**Porcentaje atacado por todo el fraude digital de COVID-19**
Canadá	Phishing	30%
Colombia	Estafas de vendedores externos en sitios web minoristas en línea legítimos	25%
Hong Kong	Phishing	37%
Sudáfrica	Estafa por desempleo	38%
Reino Unido	Phishing	30%
Estados Unidos	Phishing	31%

Fuente: (TransUnion, 2020)

Un factor que juega un papel importante es el talento humano de las organizaciones que son sujetas a estas acciones fraudulentas, las cuales en esta investigación se ha podido observar que para ALC existe una gran ventaja para los defraudadores porque la región no cuenta con expertos que tengan un preparación orientada a ciberseguridad, sin embargo, como se observa EE.UU., está mayor preparado hoy en día para hacerle frente al problema de ciberdelincuencia buscan talento que tengan desarrollado las capacidades de análisis de la informática sobre todo en levantamientos de ingeniería social, que cuenten con un equilibrio emocional, atentos a su entorno y preparación forense.

2.1.2. Microentorno

2.1.2.1. Clientes

Honduras no ha sido la excepción en cuanto a los efectos que ha generado la migración y adaptación de usuarios al ámbito digital en los medios de pagos, debido a la necesidad inminente generada durante la pandemia COVID-19 para el año 2020, el alza de transaccionalidades bajo los canales de comercios electrónicos conllevo a que tanto el sector financiero, comercial y las personas naturales y jurídicas experimentaran un aumento en los casos de cibercrimen, consistiendo éste en clonación de tarjetas de débito y crédito, extracción de información financiera, falsificación o usurpación de documentos de identificación entre otros modos operandi.

Los bancos comerciales de Honduras ofertan a sus clientes productos y servicios con facilidades de utilización en los medios de pagos, entre éstos encontramos tarjetas de crédito, tarjetas de débito y canales de transaccionalidad para hacer pagos y transferencias entre otras operaciones, haciendo uso de internet por el APP y banca por internet.

Sin embargo, a pesar de los diferentes servicios y productos que ofertan las instituciones financieras, más que generar un beneficio traen consigo la atracción de los defraudadores,

quienes utilizando tácticas y experiencias de otros países y valiéndose del desempleo de muchas personas por la crisis económica, contratan individuos para accionar el fraude utilizando falsificación de documentos, infiltración a las instituciones, permitiendo que se extraigan datos para poder hacer la ingeniería social determinada por capacidades de pago, que permiten la apertura de productos como créditos o tarjetas que dan la facilidad de obtener efectivo rápido, cuando los clientes se percatan llaman a las instituciones, sin embargo, en ocasiones resulta desfavorable al cliente, debido que a través de una llamada, redes sociales y correos los defraudadores atacan a los clientes, obteniendo claves que le permiten acceder a los canales digitales como las APP y banca por internet, saqueando sus cuentas tanto de ahorro, corrientes y disponibilidades de créditos.

2.1.2.2. Proveedores

Los proveedores estratégicos de aplicaciones, utilizadas para el proceso de monitoreo y prevención de fraudes son:

- VISA y MasterCard: son instituciones financieras multinacionales que facilitan los medios de pago a través de tarjetas de crédito y débito. Proporcionando también herramientas de soportes operativos, financieros y de negocio, en donde ponen a disposición de sus afiliados las herramientas de motor de análisis de fraude, como lo son: gestor de riesgos de Visa (VRM sus siglas en ingles) y experto monitor de soluciones (EMS sus siglas en inglés) respectivamente.
- TODO1: es una empresa financiera expertos en canales digitales, que proporciona a la institución un módulo de perfilamiento para el análisis de riesgo de las transacciones que realizan los clientes en el APP, al cual denominan IUVIPROFILER que su significado es LUVI del latín ayuda y PROFILER que en ingles significa perfilador. (TODO1, 2021)

2.1.2.3. Competidores

El Banco Central de Honduras (BCH), como regulador de la política monetaria y crediticia del país, encabeza el Sistema Financiero Nacional (SFN) que está conformado por 15 bancos comerciales de los cuales 9 son de capital extranjero y el resto nacional, 10 sociedades financieras, 2 bancos estatales y una oficina de representación, éstos están regulados por la Comisión Nacional de Banca y Seguros (CNBS) entidad de la cual emanan las normas y políticas que este sector debe de cumplir sumadas a las leyes. (CNBS, 2021)

Durante el año 2020, se empezó a observar en los distintos medios de comunicación, comentarios de personas en donde indicaban haber sido víctimas de fraudes financieros por defraudadores, para ello las instituciones financieras, iniciaron campañas para reforzar la educación financiera y explicar los cuidados que debían de tener las personas ante situaciones que podrían enfrentar y detonar en fraudes, las consecuencias van desde la materialización monetaria, riesgo reputacional y pérdida de mercado.

A mediado del año 2021, la Asociación Hondureña de Instituciones Bancaria (AHIBA) toma como iniciativa apoyar a través de acciones concretas, tanto a sus afiliados como a la población en general a través de anuncios que alertaban sobre las medidas que debían de seguir los usuarios financieros de igual manera en colaboración con el sector bancario se estableció un comité de fraude que tenía el objetivo de integrar herramientas, establecer capacitación para prevención de fraudes a las personas encargadas de estos análisis, gestionar con el gobierno la creación de reglamentos, leyes y unidades especializadas, así como compartir las mejores prácticas.

Orellana declaró:

> A pesar de la conformación del comité, el mismo no ha podido cumplir con los objetivos que se tenía, debido a la anuencia de algunas instituciones financieras de revelar datos que pudieran ser evaluados por expertos internacionales, de manera de que como país pudiéramos aportar y colaborar en las medidas mitigantes de fraudes y así reforzar nuestros sistemas, es por ello que no podemos contar con métricas, que como sector podamos hacer una ingeniería social al modo operandi de los defraudadores. (Orellana, 2021)

La banca se enfrenta a un enemigo invisible el cual cuenta con estructuras organizadas que fácilmente descubren las brechas débiles que aún tienen las instituciones bancarias, que a pesar de contar con una buena infraestructura tecnológica y con la experiencia de usuarios en términos digitales y de internet, se vuelve imposible tener conocimiento de cuándo van a ser atacados.

2.1.3. Análisis interno

2.1.3.1. Situación financiera

Según la posición del sistema bancario comercial con cifras al 31 de agosto del 2021, Davivienda ocupa la sexta posición, tanto en activos, cartera crediticia, depósitos, capital y utilidades, es el único en el sector financiero que en todos los factores evaluados se mantiene en el mismo nivel (Ver anexo No.1), en los últimos años el banco ha mostrado un crecimiento del saldo de la cartera de tarjetas de crédito que le da una participación del mercado del 10.1%, colocándolo en el nivel 4, antecedido por Banco Atlántida, Banco BAC y Ficohsa. (CNBS, 2021)

Las cifras en cuanto a clientes y de algunas operaciones que realizan, en torno al tema de esta investigación se detallan:

Tabla 3. Cantidad de clientes y operaciones por año.

	Año		
Cantidades de:	**2019**	**2020**	**A agosto 2021**
Clientes activos Digitales (APP y Banca por internet).	19,109	50,542	58,385
Clientes con Cuenta de Ahorro y Cheques.	136,440	163,885	174,350
Tarjetas de Crédito.	41,233	37,875	40,368
Tarjetas de Débito.	168,347	120,802	124,387
Operaciones con tarjetas de crédito en comercios electrónicos.	497,744	738,202	674,738
Operaciones con tarjetas de crédito en puntos de ventas.	2,202,788	1,614,666	1,802,856
Operaciones con tarjetas de débito en comercios electrónicos.	311,983	778,918	811,106
Operaciones con tarjetas de débito en puntos de ventas.	2,423,753	1,682,680	1,879,739

Fuente: (Davivienda , 2021). Elaboración propia.

2.1.3.2. Recursos Humanos

El área de Operaciones en tarjetas de Davivienda está compuesta por 28 personas, teniendo como objetivo apoyar en las actividades del negocio de medios de pagos garantizado que se tenga en forma oportuna los materiales e insumos necesarios que se requerirán en las negociaciones con el cliente de manera que se generen experiencias de alto estándares.

Dentro de esta se encuentra el departamento de monitoreo y prevención de fraude que tiene como finalidad realizar actividades del proceso de alertamientos de transacciones con potencial de fraudes, la estructura está compuesta cinco (5) analistas y un jefe.

2.1.3.3. Proceso de monitoreo de fraudes

El objetivo de este proceso es poder detectar a tiempo las transacciones, por uso de tarjeta de crédito, débito y operaciones en APP, bajo las reglas emanadas de las políticas de prevención que se establecen.

El departamento de monitoreo y prevención de fraude, es el encargado de ejecutar la contactación, que consiste en que uno de los analista de monitoreo llame al cliente para la

confirmación de la transacción ejecutada, que de igual manera conlleva un análisis de ésta, bajo estándares establecidos por el banco; al identificar un ataque de inmediato debe notificarse a la jefatura y al área de gestión integral de riesgos para que se puedan generar mitigantes de las brechas que deja ver el intento de fraude.

2.1.3.4. Proceso de atención de reclamos de consumos no reconocidos

El objetivo de éste es poder atender las quejas y reclamos de consumos u operaciones que el cliente no reconoce, a través de un análisis extensivo y haciendo uso de las herramientas que las marcas VISA y MasterCard proporcionan, así como de los sistemas de la organización.

El cliente presenta su reclamo o queja, detallando lo que él considera es un incidente o bien no reconoce la transacción o el consumo, el área de monitoreo y prevención de fraude recibe la gestión en donde el gestor de operaciones en tarjeta procede con el análisis y atención de la gestión, es importante recalcar que en caso de que sea una compra con tarjetas existe tiempo de respuesta por la intervención de las marcas VISA o MasterCard, de igual manera si el caso es considerado como fraude inicia una recopilación de información requerida para el informe y poder evaluar si hay oportunidades de mejora en temas preventivos, al concluir se remite al área de atención de usuario financiero las respuestas, para que sean ellos que formalmente den un dictamen a los clientes de su gestión.

2.1.3.5. Licenciamiento con las marcas VISA y MasterCard

Toda institución financiera que sea emisora de tarjeta de crédito suscribe un contrato de licenciamiento o franquicia para hacer uso de la marca, en este caso Davivienda en la actualidad cuenta con estas dos licencias, que le dan la oportunidad de ofertar a los clientes productos y servicios acorde a sus necesidades y a la vanguardia, estas facilidades se consideran como medios de pagos.

Ambas marcas para el otorgamiento de licencias, exigen estándares de seguridad y calidad basado en las Normas de Cumplimiento de la Industria de Tarjetas (PCI por sus siglas en inglés), de igual manera proveen de plataformas y recursos que facilitan las relaciones y usos de los servicios que prestan, dentro de las exigencias en los cuidados de las emisiones y las autorizaciones que se dan, para lo cual ambas marcas constantemente generan foros y capacitaciones, para que las instituciones mitiguen riesgos y generen cambios o mejoras en sus sistemas de acuerdo a las exigencias de mercado.

En la actualidad se cuenta con mecanismos seguros para la autenticación, al momento de hacer uso de la tarjeta de crédito, como lo es la tecnología de Chip, que consiste en un desarrollo de criterios de seguridad únicos que dan la certeza del 99%, de viabilidad en el uso, este tipo de inclusión de mejora mitigante surge a mediados del año 2014, en donde las marcas se unen al ver el alto índice de fraudes por clonación de banda dando el nombre de tecnología Europe, MasterCard y VISA (EMV por sus siglas en inglés).

El mundo de tarjetas es muy cambiante y evoluciona constantemente, es por ello que demanda especializaciones de las personas involucradas en los procesos, requiriendo habilidades técnicas y analíticas de alto nivel, las marcas de igual manera generan campañas para que los usuarios puedan tomar conciencia de la seguridad que pueden dar a sus productos como por ejemplo: no tomar fotos de sus plásticos y compartirlo, no dar información por teléfonos entre otras; igual manera hoy en día estamos migrando que todas las transacciones sean a través de tokenización, que consiste en un código de seguridad que será requerido al momento de realizar una compra o transacción; sin embargo las marcas son conscientes de la ardua tarea que se tiene con los defraudadores.

Esta investigación ha logrado obtener datos de las marcas en consideración a la involucración de uno de los miembros, sin embargo, esta información es de carácter sensitiva

y de alto grado de confiabilidad expuesta solo a usuarios con acceso a las plataformas de las marcas.

2.2.Conceptualización

Comercio electrónico

Las compras y ventas en canales digitales ponen a disposición sus productos en redes sociales o sitios web y hacen desaparecer la presencia física de un local, haciendo uso del 100% de sistemas de información y tecnología. (Martín, 2018)

Ingeniería Social

Es la acción en donde se manipula a las personas a través de técnicas y habilidades especializadas, de manera de extraer información para ser analizada y utilizada en pro o en contra de una persona. (Castellanos, 2021)

Ciberseguridad

Según la Unión Internacional de Telecomunicaciones (UTI),

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías; que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. (Destino Negocio, 2021).

Biometría:

De acuerdo con la definición de la Organización Internacional de Normalización: son las técnicas utilizadas para el reconocimiento automático de las personas, las cuales se basan en sus características físicas, naturales, así como conductuales, entre éstas se pueden nombrar: color de ojos, tipo de cabello, huellas y la silueta de su rostro. (ViaFirma, 2021)

Tokenización:

Tecnicismo utilizado en el sector financiero. Como parte de la protección a la información, se le asigna al usuario códigos que son de conocimiento único de los expertos encargados, de esta manera se evita la exposición de datos confidenciales para la organización. (Lutkevich, 2021) Afirma que: "es el proceso de reemplazar datos confidenciales con símbolos de identificación únicos, que retienen toda la información esencial sobre los datos sin comprometer su seguridad".

Inteligencia de negocio:

Son todos los procesos, tecnología y aplicaciones que ofrecen de manera más ágil y los resultados de las gestiones empresariales para que sean objeto de análisis. (Castro, 2021)

2.3.Teorías de sustento

2.3.1. Teoría General de la Administración

Las organizaciones constantemente están en busca de lograr el cumplimiento de los objetivos empresariales, mismos que son obtenidos por medio del control estratégico de los recursos y correcta ejecución de los procesos. El concepto "administración" puede ser empleado en diferentes áreas o condiciones de la empresa (Torres, 2014), cita diferentes autores que propusieron diversos conceptos en diferentes épocas y situación empresarial. En este caso, T.S. Bateman y S.A. Snell en 1990, propusieron que la administración es un "Proceso de trabajar con personas y con los recursos para alcanzar las metas de la organización".

Por lo tanto, la teoría general de la administración podría definirse como el estudio del manejo de una empresa sin importar el rubro, que hace uso de sus recursos ya sea humano o de procesos que apoyen en el adecuado desarrollo y funcionamiento de la organización. La cual cuenta con 6 principales variables: tareas, estructuras, personas, tecnología, ambiente y

competitividad. Estas variables conllevan a una interrelación sistemática y compleja, ya que cada una influye entre sí.

El proceso administrativo, es el conjunto de pasos que las empresas hacen uso para el desarrollo de la implementación de nuevas metodologías estratégicas y el logro de las mismas. Es importante recalcar que dicho proceso está dividido en dos fases: la fase mecánica y la fase dinámica. La primera, comprende dos etapas que consisten en la planificación y la organización de las tareas que se realizarán, dejando de forma clara los objetivos que se desean lograr y el orden de las asignaciones. En la segunda fase, se encuentran las etapas de ejecución de las tareas, estas son: la dirección y el control, mediante estas se toman en cuenta los márgenes de error que puedan presentarse en el desarrollo de las mismas, de igual forma, el seguimiento que se requerirá para el correcto manejo del proceso a ejecutar. (López J. , 2021)

Esta teoría, explica los aspectos exclusivos de cada asociación en donde los administradores definen estrategias, analizan soluciones, miden los recursos, buscan solucionar problemas a través de la innovación y la competitividad de su rubro. Por lo tanto, dicha teoría busca que todo proceso que involucre la creación de un producto o brindar un servicio, se requiere de constante supervisión que garanticen la efectividad en su elaboración, dicho monitoreo se realiza por medio de controles administrativos de los procesos que (Gómez, 2016) lo define como: “el proceso que permite garantizar que las actividades reales se ajusten a las actividades proyectadas”. De esta forma, las organizaciones elevan su productividad y procesos orientados al logro de metas. A la vez, Gómez establece tres tipos de control:

- Control preliminar
- Control concurrente
- Control de retroalimentación

Control preliminar: consiste en la elaboración de reglas, instrucciones o políticas que guiarán el proceso, de manera que éste sea ejecutado con menor riesgo de errores y asegurando los altos índices de éxito.

Control concurrente: evalúa el progreso de las actividades realizadas durante el proceso, así como el desempeño de los colaboradores brindando un ambiente laboral adecuado, asegurando el cumplimiento de los estándares establecidos previamente.

Control de retroalimentación: se concentra en evaluar los resultados del proceso, de esta forma, se tomarán decisiones necesarias con relación a continuar en la ejecución o regresar a un punto que refleje una alerta de falla.

Considerando la importancia de llevar de la mano los procesos internos de la empresa y el debido monitoreo adecuado a cada uno de ellos, se establece la necesidad de la implementación de controles administrativos que rijan el desarrollo de las actividades y procesos establecidos, obteniendo alertas preventivas que, a futuro podrán minimizar el grado de riesgos de la empresa, que sirvan de soporte para la toma de decisiones acertadas, y las actividades que conlleva el proceso no caen en un círculo repetitivo que a futuro alejará al cumplimiento de la meta.

De igual forma, existe un método que logra apoyar dicha teoría y es el denominado Diagrama de Ishikawa, el cual su función principal es destacar los aspectos relevantes de la situación actual de la organización, por lo tanto, se crea una visión más amplia al momento de tomar una decisión. Dicha herramienta fue creada por Kaoru Ishikawa, especialista en control de calidad, quien dio la forma de pescado al diagrama ya que era una manera más interesante de visualizar las causas de los problemas de una organización u otro ámbito por aplicar. Sin embargo, (Díaz & Romero, 2010) consideran que “esta herramienta no ofrece respuesta a una pregunta, como el análisis de Pareto, diagramas Scatter o histogramas; en el momento de

generar el diagrama causa-efecto, normalmente se ignora si estas causas son o no responsables de los efectos". Por lo que es una metodología orientada únicamente a recolectar información.

Ventajas de la Teoría General de la Administración:

- Mejora en la ejecución de estrategias y procesos de la organización.
- Mejora en la toma de decisiones, ya que genera un panorama más amplio acerca de la situación actual de la empresa.
- Menor índice de error y riesgos de la empresa.

Desventajas de la Teoría General de la Administración:

- Evalúa aspectos de proceso y organizacionales, mas no del desempeño del colaborador.
- Requiere constante actualización por personal especializado, por lo tanto, no existe participación del total de la empresa.

Según Katz, dentro del proceso administrativo, adicional a los factores y variables, se deben agregar las habilidades que son prioritarias para que el mismo sea exitoso, entre ellas menciona:

- Habilidad Técnica: es la capacidad de ejecutar tareas o actividades basadas en conocimientos especializados.
- Habilidades Humanas: es la relación interpersonal entre una o más personas y la capacidad de interactuar entre sí.
- Habilidad conceptual: conjunto de la visión o unidad organizacional que facilita idear, conceptualizar, establecer teorías y abstracciones. (Chiabenato, 2008)

2.3.2. Teoría sobre la Seguridad Informática

Son innumerables las ventajas y beneficios que en la actualidad los seres humanos enfrentan ante los avances tecnológicos en todas las áreas de su vida, pero también es importante recalcar el hecho que a medida que las personas tengan más acceso a plataformas digitales, el riesgo a sufrir un ataque o robo de información cibernética aumenta. Según un estudio realizado, el concepto de seguridad informática lo define como:

> El aseguramiento de la información (IA) consiste en la gestión de riesgos relacionados con el uso, los procesamientos el almacenamiento y la transmisión de información o datos, y con los sistemas y procesos empleados en la realización de esas actividades. (López C. , 2019).

Por lo tanto, toda organización siempre buscará la manera más efectiva para lograr proteger la información tanto interna como de sus consumidores o clientes y, en el caso de instituciones financieras, es primordial la importancia de mantener resguardada la información vital de la institución.

Ante lo planteado, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) logra asegurar la información confidencial de una institución, siempre tomando en cuenta que no existe un sistema que ofrezca una protección garantizada al cien por ciento. Sin embargo, Williams Deming plantea que dicho sistema puede ser a través de un proceso cíclico denominado PHVA:

- Planificar. En esta etapa se deben cumplir las siguientes acciones:
    - Determinar el alcance del SGSI en términos de negocio, la empresa, su localización, activos y tecnologías.
    - Fijar una política de seguridad.
    - Identificar, analizar y evaluar los riesgos.
    - Evaluar alternativas de tratamiento de riesgos para aplicar controles adecuados.

    - Definir una declaración de aplicabilidad que incluya los objetivos de los controles mencionados.
- Hacer. En esta fase, se realiza la implementación del Sistema de Gestión de Seguridad de la Información. Para lo cual, se deben tomar decisiones como:
    - Establecer e implantar un plan de tratamiento de riesgos.
    - Implementar los controles anteriormente seleccionados.
    - Definir un sistema de métricas para medir la eficacia de los controles.
    - Implantar procedimientos para detectar y resolver los incidentes de seguridad.
- Verificar. Abarca las tareas para la monitorización del SGSI, las cuales son:
    - Revisar regularmente la efectividad del sistema.
    - Medir la efectividad de los controles planteados.
    - Actualizar los planes de seguridad.
    - Revisar las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables.
    - Realizar periódicamente auditorías internas del SGSI.
- Actuar. Las acciones que se desarrollan en esta fase deben darse regularmente. De lo contrario, los resultados no serán favorables. Deming nombra las siguientes:
    - Instaurar las mejoras a identificar en el SGSI.
    - Comunicar las mejoras a todas las partes interesadas con detalles y precisión.
    - Garantizar que las mejoras implantadas logren los objetivos previstos. (citado por (Molina, 2019)

En conclusión, las altas demandas del uso de plataformas digitales han convertido o expuesto la información personal, financiera y emocional de las personas, de tal manera que los fraudes digitales y actos delictivos en estas plataformas son más frecuentes. Por lo que lleva

a las empresas a hacer uso de estos sistemas de protección que brinden confiabilidad ante los clientes.

Ventajas:

- Asegurar la información de las personas que dan uso diario a plataformas digitales.
- Disminución de índices o ataques digitales relacionados a fraudes.
- Brindar confiabilidad a los nuevos usuarios al consumo de plataformas digitales.

Desventajas:

- No aseguran el cien por ciento de efectividad.
- Surgen nuevas plataformas digitales, por lo que no se alcanza a cubrir el total de las amenazas.

2.3.3. Teoría de Gestión de Tecnología e Innovación

La tecnología ha sido un fiel acompañante del avance y desarrollo del ser humano, con el tiempo han surgido nuevos aportes tecnológicos que facilitan la cotidianeidad de las personas en sus actividades varias. Por lo tanto, la gestión de tecnología según (Ortíz & Nagles García, 2013) lo define como un "proceso de administración, adquisición, implementación y difusión de esta, en diferentes sectores, entre ellos el industrial y de servicios o el público y privado". Pero, para lograr comprender este avance y las consecuencias del mismo, es importante conceptualizar tecnología e innovación.

Tecnología: "Es un saber experto basado en el conocimiento científico o en el propio dominio de la tecnología que se ocupa de investigar, diseñar artefactos y planear su realización, operación y mantenimiento, apoyado siempre en el saber de una o más ciencias" (García, 2015)

Innovación: Joseph Schumpeter propuso que la innovación "Es la introducción en el mercado de un nuevo producto o proceso, capaz de aportar algún elemento diferenciador, la apertura de un nuevo mercado o el descubrimiento de una nueva fuente de materias primas o productos intermedios". (Díaz & Espinoza, 2018)

Para gestionar la tecnología e innovación de una empresa requiere de un proceso de 5 pasos que según (Ortíz & Nagles García, 2013) son los siguientes:

- Identificación de la tecnología: detectar fuentes portadoras de conocimiento, desde los ambientes externos e internos que resulten útiles para establecer, mantener y promover constantemente la innovación en la empresa.
- Selección del rumbo tecnológico: marca la ruta tecnológica por seguir, para afrontar su desarrollo en el corto, mediano y largo plazo.
- Acceso a la tecnología: establece la forma en cómo la empresa decide estratégicamente obtener la tecnología que resulta de su interés.
- Explotación de la tecnología: busca que se dé la explotación de la tecnología a través de la generación de capacidades, que permitan no sólo recaudar las inversiones, que por la vía de las adquisiciones de tecnología se hayan dado en el pasado, sino hacer de la misma una opción de negocio, si se lo propone estratégicamente la empresa.
- Protección de la tecnología: La tecnología se convierte en fuente de ventaja competitiva para la empresa gracias a las innovaciones; es decir, que el nuevo conocimiento generado, debe ser objeto de protección en lo posible, ejerciendo los derechos de propiedad intelectual.

Puesto que la tecnología es una ciencia que avanza y con ella los procesos involucrados en las organizaciones, se ve la necesidad de la gestión de tecnologías e innovación con el fin de evitar afectar diversos factores de la empresa.

Algunos autores plantean lo siguiente:

> Para las empresas, es fundamental el gestionar la tecnología, ya que de esta manera evitan riesgos de pérdidas causadas por la falta de agilidad en los procesos. De igual

> forma, partiendo de la constante búsqueda de satisfacción del cliente, perciben la necesidad de innovar en sus productos o servicios. (Ortíz & Nagles García, 2013, pág. 108)

Ventajas:

- La tecnología está en constante actualización, lo que trae consigo diversas novedades en todas las áreas.
- Actualización de procesos en las organizaciones conforme a las nuevas tendencias.
- Obtiene resultados en menor tiempo y acertados.

Desventajas:

- No todas las organizaciones tienen la oportunidad de tener el acceso a las nuevas tendencias y tecnologías.
- Requiere de personal especializado para la ejecución de nuevos procesos lo que causa la necesidad de nuevos contratos.
- La implementación de nuevas tecnologías podría reducir el personal provocando despidos.

2.4. Metodología aplicada

Esta investigación, ha considerado la teoría general de la administración para apoyo en el desarrollo, por lo que se ha tomado de referencia la tesis de postgrado de los maestrantes Wilford Davis y Roger Vélez de la Universidad Tecnológica Centroamericana (UNITEC), con el tema “Iniciativa para mejorar la gestión de cobranza en Banco Davivienda” en el año 2018, el objetivo de esta iniciativa fue valorar la implementación y la evaluación en la propuesta de mejora a la necesidad de nuevas estratégicas de cobranzas, que ayudarán a la reducción de gastos administrativos generadas por la operación, así como la disminución de fondos de

reserva por el constante incremento de la morosidad de la cartera de clientes, por medio de la tercerización de la cobranza con empresas dedicadas a dicha actividad.

Con la implementación de la subcontratación (Outsourcing), se refleja una reducción considerable en todos los gastos administrativos asociados a la operación, tales como sueldos, comisiones, mantenimientos entre otros, siendo este un impacto económico positivo para la institución, a lo cual se suma la liberación de reservas por obligaciones patronales y crediticias.

Adicional se obtuvo mejoras en los niveles de morosidad por la implementación de estrategias y metodologías, que apoyan la medición de los costos de productividad del personal a cargo de la cobranza, maximizando todos los recursos con el objetivo de tener una mejora y estabilidad en los resultados.

Este tipo de evaluaciones permitió a la empresa Outsourcing, brindar a la institución recursos competentes y capacitados para realizar las labores indicadas, así como poner a disposición la experiencia en la recuperación de créditos en mora.

Sin embargo, en la búsqueda no se pudieron detectar algunas investigaciones que mencionaran su aplicación y que la misma tuviera éxito, es por ello que solamente se documenta la expuesta anteriormente.

2.5.Marco legal

A manera de sintetizar las leyes que esta investigación ha indagado, se identificaron los capítulos y artículos de las mismas haciendo de éstos una explicación propia.

Tabla 4. Matriz de leyes aplicables.

LEY DE TARJETAS DE CRÉDITO (La Gaceta, 2017)		
Capítulo	**Artículo**	**Descripción**
8	46	**Incumplimientos de los Establecimientos Comerciales Afiliados.** Se rige bajo la responsabilidad que se le es asignada a la institución emisora en casos de transacciones dudosas o sin consentimiento del Tarjeta-Habiente.

Continuidad de tabla

11	54 y 55	**Programa de Educación Financiera.** El objetivo principal del presente artículo es detallar las condiciones y la necesidad de crear un programa de capacitación financiera, respetando fechas, estructura y participantes del mismo, con el fin de brindar información suficiente al Tarjeta-habiente del servicio o producto brindado.
Artículo 38-A		Tiene como objetivo proteger el uso confiable de la tarjeta de crédito, condenando todo acto que se efectúe sin el consentimiento del Tarjetahabiente. De igual forma, delimita la intervención y responsabilidad de la institución financiera con respecto a lo antes mencionado.
12	57	**Procedimiento para Presentación de Reclamos.** Recalca la importancia de la atención brindada con relación a dudas o reclamos realizados por el Tarjeta-Habiente, haciendo énfasis en la cobertura de la misma y ofreciendo soluciones o respuestas según los lineamientos establecidos.
	58	**Registros a Disposición de la CNBS.** Enmarca de manera puntual el control de registros de documentación financiera, que deberán ser presentados ante la CNBS y las especificaciones que ésta enfatice o requiera.
CODIGO PENAL (Gaceta, 2019)		
5	365	**Estafa.** Resume tres tipos de estafa que son castigadas con prisión de 2 a 4 años si éste supera la cantidad de 5mil lempiras, en los cuales se detalla que todo individuo que intente o ejecute el acto de obtener beneficio ilícito a través de engaño o manipulación, ya sea transferencias sin consentimiento, uso ilegal de documentos personales a nombre de otra persona con ánimos de lucro; es considerado estafa lo que recibe el castigo antes mencionado.
NORMAS COMPLEMENTARIAS PARA EL FORTALECIMIENTO DE LA TRANSPARENCIA, LA CULTURA FINANCIERA Y LA ATENCIÓN AL USUARIO FINANCIERO. (CNBS, 2012)		
1	5	**Obligaciones del usuario financiero.** Hace hincapié en las normas que deben ser cumplidas por el usuario ante el consumo de servicios o productos financieros, a la vez, hacer de su conocimiento las condiciones de los mismos.
	8	**Transparencia de la información.** La información ofrecida por las instituciones financieras debe ser completa, clara, sin omitir detalles. De esta forma, se asegura el consentimiento del usuario financiero ante el consumo de los servicios y productos.
	9	**Área de atención de los reclamos.** Toda institución financiera debe tener un área dedicada exclusivamente para atender reclamos y consultas por parte de los clientes, ofreciéndoles la información y respuestas según el caso que corresponda.
4	15	**Informar sobre las condiciones contractuales, derechos y obligaciones de los usuarios financieros.** Las condiciones, políticas y detalles correspondientes a los contratos de servicios o productos financieros, deben ser compartida con los usuarios de manera clara y detallada
6	18	**Sistema de atención al usuario financiero.** Dicho artículo tiene como objetivo resaltar que toda institución financiera debe tener un sistema de atención al usuario, que cumpla con los requerimientos necesarios para responder las consultas del cliente.

Elaboración propia.

CAPITULO III. METODOLOGÍA

3.1.Congruencia metodológica

3.1.1. Matriz metodológica

Titulo	Problema	Preguntas de investigación	Objetivos		Variables	
			General	**Específicos**	**Dependiente**	**Independientes**
Propuesta de herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras.	Incremento en alertas de monitoreo y prevención de fraudes en el análisis y confirmación con los clientes.	¿Culés son los factores que influyen en el proceso ejecutado por Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios?	Proponer los requerimientos necesarios para una herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras, mediante la indagación de la tecnología, controles y la experiencia de personas involucrados en el proceso y tema, para apoyar en la eficiencia de los controles de riesgos operativos y el servicio al cliente, así como el mantenimiento de una carga laboral óptima.	Conocer los factores que influyen en el proceso ejecutado por Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.	Factores	Motores de análisis Comportamiento transaccional
		¿Cuáles son los requerimientos regulatorios, políticas y técnicos necesarios para establecer un sistema que pueda utilizar Davivienda para la prevención de fraudes en los canales digitales y comercios?		Determinar los requerimientos técnicos, regulatorios y políticas que debe de contener un sistema de información que Davivienda pueda utilizar para la prevención de fraudes en los canales digitales y comercios.	Requerimientos técnicos regulatorios y políticas.	Reglas Reformas Aplicabilidad
		¿Cómo el proceso de gestión de tecnología e innovación puede apoyar en establecer una herramienta integradora que pueda utilizar Davivienda para la prevención de fraudes en los canales digitales y comercios?		Considerar el proceso de gestión de tecnología e innovación para la propuesta de una herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.	Proceso de gestión de tecnología.	Sistemas de seguridad. Controles Personas
		¿Cómo plantear el diseño de una propuesta para una herramienta integradora que pueda utilizar Davivienda para la prevención de fraudes en los canales digitales y comercios?		Plantear el diseño de una propuesta de herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.	Herramienta integradora.	Soluciones Diseño Experiencia.

Tabla 5.Matriz metodológica.

3.1.2. Esquema de variables de estudio

La presente investigación tuvo como objetivo proponer los requerimientos necesarios para una herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras que pueda apoyar la eficiencia en el proceso.

Para esta investigación se identificaron las siguientes variables:

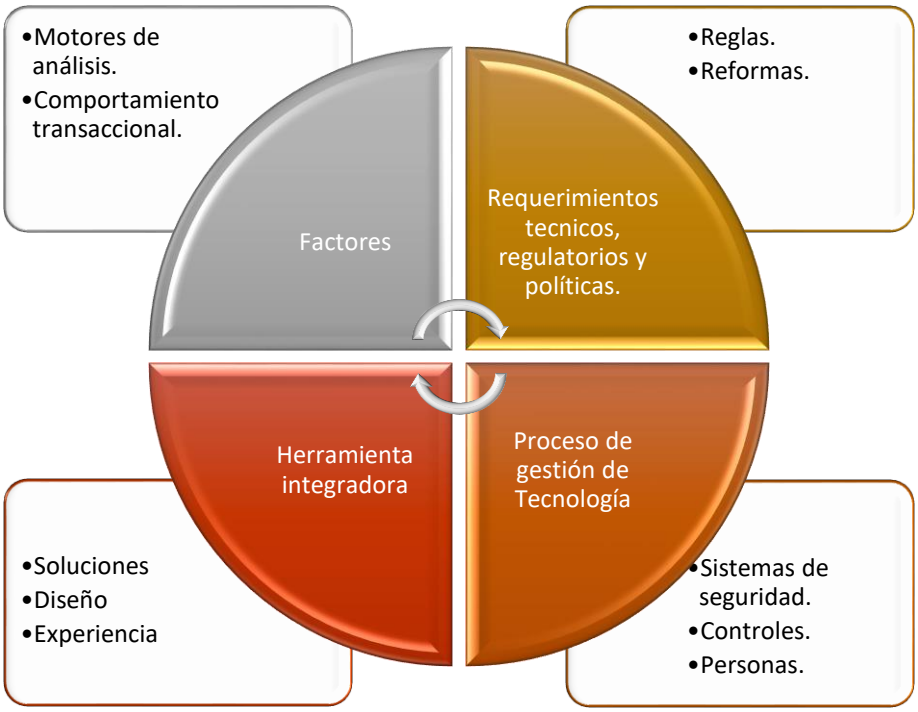
Variable Independiente:

- Motores de análisis
- Comportamiento transaccional
- Reglas
- Reformas
- Sistemas de seguridad
- Controles
- Personas.
- Soluciones
- Diseño
- Experiencia

Variable Dependiente:

- Factores.
- Requerimientos técnicos, regulatorios y políticos
- Proceso de gestión de la tecnología.
- Herramienta integradora.

Figura 1. Esquema de variables de estudio.



Elaboración propia.

3.1.3. Operacionalización de las variables.

PROPUESTA DE HERRAMIENTA INTEGRADORA DE ANÁLISIS Y PREVENCIÓN DE FRAUDE PARA BANCO DAVIVIENDA HONDURAS							
	Definición						
Variables Independientes:	**Conceptual**	**Operacional**	**Dimensión**	**Indicador**	**Ítem**	**Unidades (Categorías)**	**Escala**
Motores de análisis	Plataformas en línea sólida, que gestiona las normas en tiempo real para rechazar o alertar aprobaciones de operaciones, identificando sospechas que requieren una mayor investigación.	Es el conjunto de herramientas y parámetros, que interactúan entre sí para la obtención de alertas y datos necesarios, para el análisis y monitoreo de transacciones con sospechas de fraudes.	Tecnología utilizada. Parámetros Generación de datos.	Herramientas	1. ¿Cuáles son las herramientas que se utilizan en el proceso de análisis y prevención de fraudes?	No Aplica	Preguntas abiertas
Comportamiento transaccional	Conjunto de conductas y conocimientos propios de una persona, que puede determinar o predecir un evento en la manera de usar su producto o servicio.	Secuencia que resulta al momento que los clientes realizan o usan los diferentes canales que el banco pone a su disposición, de manera que puedan hacer uso de sus productos.			2. ¿Conoce usted una herramienta ya existente en la industria o mercado que integre lo expuesto anteriormente? ¿Si los hay podría compartir el nombre de empresas que prestan este servicio?		
					3. ¿Cuáles son los datos mínimos requeridos para el análisis de una alerta?		
Reglas	Conjunto de medidas que supervisan y delimitan la correcta aplicabilidad de los procesos o acciones, establecidas para garantizar la eficiencia y mitigación de riesgos.	Medidas de monitoreo que vigilan la correcta aplicabilidad de los procesos, bajo las políticas, normas y regulaciones establecidas, con el fin de mitigar las alertas de fraude en canales digitales y comercio.	Políticas. Regulaciones. Normas.	Políticas, Regulaciones y Normas Existentes	4. ¿Cuáles son las políticas, regulaciones y normas que considera en un proceso de monitoreo y prevención de fraudes?	No Aplica	Preguntas abiertas
Reformas	Es la modificación de disposiciones legales contenidas en un código o ley.	Cambios que surgen en el tiempo, posterior a la divulgación de una ley o código de manera de adecuarla al tiempo actual.					

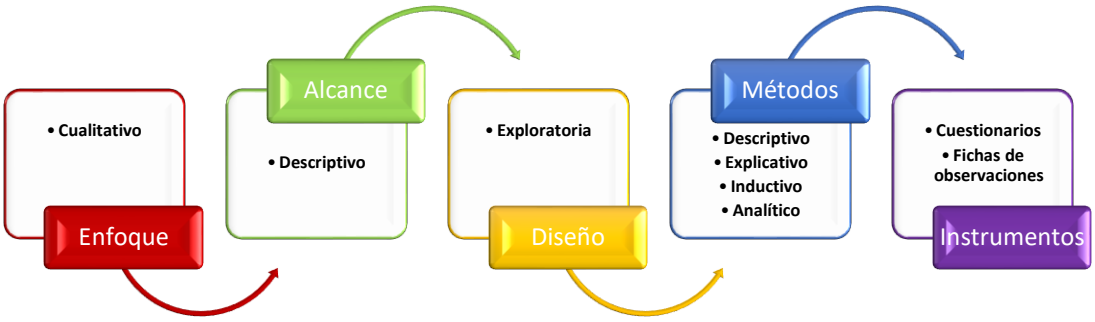
Continuidad de tabla

Sistema de Seguridad	Grupos de elementos instalados e intercomunicados entre sí que previenen, detectan o actúan ante una amenaza.	Factores relacionados entre sí, que tienen como objetivo común, prever amenazas de fraudes o robo de información	Conocimientos y habilidades. Factores, practicas o técnicas	Detalles de habilidades	5. ¿Cuáles son las métricas que se generan para la evaluación del proceso de monitoreo y prevención de fraudes?	No Aplica	Preguntas abiertas
Controles	Observación cuidadosa que sirve para hacer una comprobación.	Supervisión de los elementos involucrados en el proceso de análisis y prevención de fraudes			6. ¿Qué factores o elementos deben de conjugar en una herramienta de monitoreo y prevención de fraudes?		
Personas	Individuos que tiene la capacidad de interactuar y adquirir conocimientos.	Ser humano racional que tiene la capacidad de analizar una alerta, así como para generar experiencias vividas.			7. ¿De acuerdo con su experiencia, qué prácticas y técnicas considera que debe de tener una herramienta de prevención de fraudes?		
Soluciones	Respuesta eficaz a un problema, duda o cuestión.	Mejoras que ayuden a resolver debilidades, identificadas en el análisis de alertamientos de fraude.	Problemática. Posibles Soluciones	Causas Propuestas	8. ¿Qué problemas considera usted se tiene en el proceso de monitoreo y prevención de fraudes?	No Aplica	Preguntas Abiertas
Diseño	Proyección de objetos útiles estéticos, que faciliten el desarrollo de un producto o servicio.	Prototipo que proporciona soluciones eficientes para la propuesta de una herramienta.			9. ¿Qué propuestas y recomendaciones podría usted dar para una herramienta integradora de análisis y monitoreo de fraude?	No Aplica	
Experiencia	Conocimiento de algo, o habilidad para ello, que se adquiere durante el tiempo de haberlo realizado, vivido, sentido una o más veces.	Conjunto de habilidades y conocimientos técnicos y analíticos que una persona ha adquirido, permitiéndole así generar opinión sobre un tema o caso.			10. ¿Considera usted importante tener una herramienta integradora donde se concentren los diferentes factores del proceso de monitoreo y prevención de fraude, así como tecnología involucradas en inteligencia de negocio?	No Aplica	

Tabla 6. Operacionalización de variables

3.2.Enfoque y métodos

Figura 2. Diagrama de elementos de la investigación.



Elaboración propia.

Explicación de los elementos del diagrama de métodos y enfoque:

3.2.1. Enfoque

La presente investigación se realizó bajo un enfoque cualitativo, partiendo de la definición aportada por (Sampieri, Fernández, & Baptista, 2014), asegura que: "el método cualitativo utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación". Por lo que, se recopiló información a partir de la observación, experiencia de expertos e involucrados en el proceso y datos brindados por Banco Davivienda, mismos que fueron objeto de análisis.

3.2.2. Alcance.

La investigación posee una orientación de tipo descriptiva, ya que tuvo como fin describir los aspectos y procedimientos relacionados al análisis de prevención de fraude

ejecutado por Davivienda Honduras, con el fin de analizar a través de entrevistas y fichas de observación en las que se registraron detalles del proceso antes mencionado. “Busca especificar propiedades y características importantes de cualquier fenómeno que se analice”. (Sampieri, Fernández, & Baptista, 2014)

3.2.3. Diseño

Se considera la investigación bajo el diseño transaccional exploratorio, ya que se indagó en un tema poco conocido y se analizó desde el inicio del proceso de análisis, tomando como referencia el concepto recuperado de (Sampieri, Fernández, & Baptista, 2014) afirman que: “es comenzar a conocer una variable o un conjunto de variables, una comunidad, un contexto, un evento, una situación. Se trata de una exploración inicial en un momento específico”.

3.2.4. Métodos

Tomando en cuenta que la investigación se realizó bajo un diseño exploratorio, el método que guió a la misma fue descriptivo, explicativo, inductivo y analítico; ya que se analizaron los procesos de prevención de fraudes y las implicaciones del mismo. Se tomó de referencia la información recopilada durante la ejecución, que consistió en la experiencia y conocimientos de expertos en el tema, como también datos proporcionados por el banco.

3.3.Diseño de la investigación

3.3.1. Población

La población de la presente investigación estuvo comprendida por 11 profesionales con experiencia tanto en análisis de fraudes, como algunos que intervienen activamente en el proceso ejecutado en Davivienda; de igual manera se consideró un

consultor con amplia experiencia en desarrollos de sistemas de información para medios de pagos.

3.3.2. Censo

En consideración al tamaño de la población, se determinó realizar un censo conformada por 11 profesionales detallados a continuación:

Tabla 7. Matriz de expertos de la población.

Profesional	Cantidad
Jefe de monitoreo y prevención de fraude	1
Analistas de Monitoreo y prevención de fraudes	5
Expertos en el tema de Davivienda regional	2
Desarrollador de sistemas de información para medios de pagos	1
Ejecutivo de riesgo transaccional	1
Subdirector de tecnología	1

Elaboración propia.

3.4. Instrumentos, técnicas y procedimientos aplicados

3.4.1. Técnicas

Con la finalidad de obtener la recolección de información, se realizó una entrevista a los profesionales con experiencia y ejecutores que participan en el proceso de monitoreo y prevención de fraudes en Davivienda, como también especialista en desarrollos de sistemas de información para los productos de medios de pagos; de igual forma se realizó una observación en la ejecución del proceso en conjunto con los analistas.

3.4.2. Instrumentos

Con el objetivo de enriquecer la investigación por medio de la recolección de información y datos, fueron utilizados los siguientes instrumentos:

3.4.2.1. Entrevista

Se elaboró una guía de entrevista (ver anexo 2) que estaba conformada por 4 preguntas generales y 10 abiertas, que se aplicaron a los analistas y al jefe de monitoreo y prevención de fraude, al ejecutivo de riesgo transaccional, subdirectora de tecnología todos ellos de Davivienda Honduras, al jefe de monitoreo y prevención de fraude de Davivienda Costa Rica, Coordinador regional de riesgo transaccional de Davivienda Colombia y al gerente de desarrollo de sistemas de la empresa Solution Technology. Con el fin de obtener información relacionada a los objetivos y aportes para la realización del proyecto. Todas las preguntas fueron abiertas y no contenían una medición de escala.

3.4.2.2. Observación

Se elaboró una ficha de observación (ver anexo 3) para el proceso de monitoreo y prevención de fraude, la cual se completó con los cinco (5) analistas, asegurando con esto obtener datos e información necesaria que permitieron profundizar en el tema y en la identificación de factores que apoyaron la propuesta de esta investigación.

3.4.3. Procedimientos

Para la aplicación de las entrevistas y ejecución de la observación, se tuvo la aprobación por parte de la dirección de operaciones y tecnología de Banco Davivienda Honduras, así como la colaboración de los diferentes profesionales y expertos, explicándoles en qué consiste la investigación, su alcance y objetivo, colocándolos así en contexto de la propuesta.

Para la ejecución de los instrumentos antes mencionados, se realizó de la siguiente manera:

- Se aplicaron las entrevistas, las cuales se agendaron de acuerdo con los tiempos disponibles de parte de los entrevistados.

- Durante el período de 3 días a partir del 10 de noviembre 2021, se realizó la observación a las actividades del proceso de análisis y monitoreo de fraudes ejecutados por los analistas, en los diferentes turnos.
- Las entrevistas y observaciones por temas de distanciamiento social se llevaron a cabo mediante videoconferencias.
- Se organizó y transcribió la información.
- Se realizó el análisis de la información y datos.
- Se realizó un resumen ejecutivo de los hallazgos.

3.5.Fuentes de Información

3.5.1. Fuentes primarias

Se realizó una entrevista al jefe de monitoreo y prevención de fraude, cinco (5) analistas de monitoreo y prevención de fraudes, tres (3) expertos en el tema, a un ejecutivo de riesgo transaccional, al gerente de seguridad de sistemas y al subdirector de tecnología.

Se recopilaron datos que provienen de la observación realizada a las actividades ejecutadas por los cinco (5) analistas de monitoreo y prevención de fraudes en el proceso, utilizando para ello el formato de ficha.

3.5.2. Fuentes secundarias

La investigación utilizó fuentes secundarias como:

- Sitios web, métricas, libros, revistas, leyes, normas y códigos.
- Manuales de instrucciones departamentales de monitoreo y prevención de fraudes.
- De igual manera, la elaboración de la presente investigación se apoyó bajo los parámetros establecidos en los Manuales de forma y fondo otorgados por la UNITEC.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

4.1.Informe de Proceso de Recolección de datos.

Para la recopilación de datos, se utilizó la técnica de entrevista, a través de una guía de preguntas, en la cual se aplicaron a 11 personas con conocimiento en el tema, de manera que permitiera obtener información relevante para la investigación, estas personas son ejecutores internos del proceso, así como tres personas externas con años de experiencia.

De igual forma se utilizó la técnica de observación, a través del instrumento que se denominó ficha de observación, este actividad se realizó en una forma agendada durante 5 días, la cual comprendía acompañar a los analistas de monitoreo y prevención de fraudes en sus actividades diarias, durante ese acompañamiento se tomó tiempos de ejecución para cada actividad, obteniendo ampliación de los conocimiento del tema para los investigadores, así como determinar puntos de mejoras que se podrían incorporar en la propuesta.

El análisis de los datos recolectados se realizó mediante resumen y clasificación de la información obtenida; planteando éste por las variables, sus indicadores y la correlación de las preguntas de la entrevista, más los aportes de la ficha de observación.

Durante la ejecución de los instrumentos, los entrevistados proporcionaron información adicional, como lo son políticas, inventario de alertas, métricas, encuestas de satisfacción de clientes y un estudio sobre la carga laboral realizado a los analistas de monitoreo; misma que se analizó a manera de generar aportes adicionales a la investigación.

4.2.Resultados de los instrumentos

4.2.1. Resultados de la entrevista

Se programó la cantidad de 12, entrevistas de las cuales se desarrollaron 11, obteniendo una tasa de respuesta del 91.66%, los datos generales de ellos se detallan a continuación:

Tabla 8. Datos generales de los entrevistados.

No.	Puesto	Empresa	Fecha Entrevista	Años de Experiencia
1	Jefe de monitorio y prevención de Fraude	Davivienda Honduras	15-nov-21	3 años
2	Analista de monitoreo de fraude		12-nov-21	7 años
3			13-nov-21	2 años
4			14-nov-21	1 año, 6 meses
5			13-nov-21	4 años
6			15-nov-21	5 años
7	Ejecutivo de riesgo transaccional		16-nov-21	6 años
8	Subdirector de tecnología		18-nov-21	32 años
9	Jefe de monitorio y prevención	Davivienda Costa Rica	19-nov-21	25 años
10	Coordinador regional de riesgo transaccional	Davivienda Colombia	12-nov-21	11 años
11	Gerente de desarrollo de sistemas	Solution Technology	15-nov-21	20 años

Fuente: creación propia

Resumen de entrevistas

1. ¿Cuáles son las herramientas que se utilizan en el proceso de análisis y prevención de fraudes?

   R. / Los entrevistados mencionaron las siguientes herramientas: VRM, EMS, IUVPROFILER, sistema bancario computarizado integrado en un sistema (ICBS sus siglas en inglés), sistema computarizado para tarjetas de crédito (SISCARD sus nombre comercial), sistema de lenguaje de consulta estructurada (SQL sus siglas en inglés), centro de contacto con el cliente (CCC sus siglas en inglés), acrónimo en los mensajes de texto para una consulta (QRY sus siglas en inglés), correo electrónico, herramientas Google y Excel.

2. ¿Conoce usted una herramienta ya existente en la industria o mercado que integre lo expuesto anteriormente? ¿Si los hay podría compartir el nombre de empresas que prestan este servicio?

   R. / 9 entrevistados afirmaron no conocer y 2 si, estos últimos detallaron que las que conocen hace parte del trabajo, pero unificado, lo que es producto de tarjetas de crédito sin importar la marca.

3. ¿Cuáles son los datos mínimos requeridos para el análisis de una alerta?
   R. /
   - Marcador de riesgo.
   - Montos de la transacción u operación.
   - Tipo de comercio presente o no presente como lo son comercios electrónicos.
   - Si la transacción es un cargo recurrente.
   - Detalle histórico de las transacciones realizadas por el cliente en los últimos 3 meses como mínimo.
   - Número de tarjeta.
   - Información básica del cliente: teléfonos, número de identidad y dirección.
   - Tipo o motivo de alerta.
   - El código de usuario que el cliente utiliza en APP o banca en línea.
   - Velocidad de transacción.
   - Cantidad de transacciones promedios que hace el cliente por día.
   - Tipo de producto de la tarjeta.
   - Fecha de la transacción.
   - Si con anterioridad ha atendido transacciones aprobadas en ese comercio.
   - Límite de tarjeta.

- Disponibilidad de su producto que está saliendo alertado, sea tarjeta de crédito o cuentas que son las relacionas en tarjeta de débito o bien en su APP.
- Fechas de aperturas del producto.
- Si tiene adicionales o beneficiarios en sus productos pasivos.
- Localización de la transacción y de número de terminal (IP sus siglas en inglés), que está utilizando en el caso de que la transacción sea en línea o APP.
- IP históricas utilizadas cuando la transacción es en el APP.

4. ¿Cuáles son las políticas, regulaciones y normas que se considera en un proceso de monitoreo y prevención de fraudes?

   R. / Políticas de riesgo transaccional para medios de pagos; en cuanto a regulaciones serian: la norma denominada conozca su cliente, ley de tarjeta de crédito, ley de usuario financiero.

   De igual manera 3 de los analistas indicaron que no conocen las políticas del proceso, en cuanto a los entrevistados externos indicaron que, no existen regulaciones internacionales que ellos conozcan que intervengan en este tipo de proceso.

5. ¿Cuáles son las métricas que se generan para la evaluación del proceso de monitoreo y prevención de fraudes?

   R. / Los que se generan son: Indicadores falso positivo, transacciones fraudulentas aprobadas, cantidad de gestiones atendidas, cantidad de alertas atendidas y pendientes, monto de fraude evitado, cantidad de transacciones declinadas, efectividad de alertas.

Indicaron que la información se trabaja bajando información de las diferentes herramientas y sistemas, la misma es adecuada en formatos de presentación tanto para el área como para otras del banco, esta información conlleva un análisis de datos ya que los utilizan para evaluar eficiencia, así como otras cosas que apoyan a estrategias del banco, es algo complejo trabajar estas datas.

6. ¿Qué factores o elementos deben de conjugar en una herramienta de monitoreo y prevención de fraudes?

   R. / Uno de los entrevistados no supo qué responder y se limitó a decir "varios" sin embargo, los demás detallaron:

   - Análisis previo.
   - Que se puedan identificar no solo transacciones que salen en alertas, sino otras que al final resultan fraude.
   - Agilidad
   - Eficiencia
   - Cantidad de transacciones consecutivas.
   - Motor inteligente.
   - Comportamiento transaccional de los clientes.
   - El gusto de los clientes.
   - Logaritmos que detecten comportamientos de clientes.
   - Conocer todos los productos pasivos y activos del cliente.
   - Comportamiento crediticio del cliente.
   - Los flujos promedios en sus cuentas activas.
   - Que los sistemas y herramientas que se utilizan estén respaldadas por proveedores de experiencia y que ellos garanticen la seguridad de los mismos.

7. ¿De acuerdo con su experiencia, qué prácticas y técnicas considera que debe de tener una herramienta de prevención de fraudes?

   R. /

   - Capacidad de ir afinando las alertas.
   - Toda la información básica del cliente.
   - Que sea en 100% en línea.
   - Que no se tenga que utilizar tantos sistemas.
   - Comportamiento de los clientes.
   - Relación de clientes en otros bancos.
   - Identificar las alertas falsas.
   - Que evalúe las actividades de los riesgos anteriores con la actual.
   - Identificar si el cliente está comprometido en listas negras por ser recurrente en fraudes.
   - Un marcador de riegos bien medido.
   - Que si el cliente tiene aviso de viaje, que los correlacionen con el lugar donde se realizó la transacción.
   - Que determine qué y cómo puedo validar la transacción sea por APP u otros canales.
   - Que se le envíe un mensaje de texto al cliente, que su producto está bloqueado por análisis de fraude y que debe de abocarse al banco.
   - Que el cliente pueda autenticar o confirmar sus alertas a través de medios tecnológicos con uso de biometría.
   - Identificar como estamos posicionados a nivel de fraude, tanto en declinaciones como en alertamientos.

- Que muestre los horarios, días picos y que realice una proyección para los próximos días.
- Gráficos de eficiencia tanto de la alerta como de atención por los analistas.
- Fácil de manejar.
- Que quien la usa pueda entender todos los elementos que se muestran.
- Enfocados en el servicio a las personas.
- Perfiles para las personas que la van a utilizar.
- Que muestre un perfil del cliente.

8. ¿Qué problemas considera usted se tiene en el proceso de monitoreo y prevención de fraudes?

   R. /

   - La capacidad de internet que se tiene en las casas, ahora que estamos en teletrabajo.
   - La desconcentración en el análisis.
   - Que las reglas no se pueden modificar, si no están autorizadas por el área de gestión integral de riesgos.
   - La experiencia de otras áreas en el tema de fraude es muy poca.
   - Poco tiempo para el análisis de alertas.
   - El no saber experiencias de otros y las prácticas de defraudadores en otras zonas, no permite poder identificar los patrones de fraudes a los que podemos estar expuestos.
   - Los analistas son ejecutores de las actividades, pero no tiene preparación para realizar un verdadero análisis profundo.
   - La cultura de nuestro país no permite adaptarnos fácil a tecnologías más seguras tanto en tarjetas, como en los otros canales.

- La falsificación de documento hace que se entreguen productos a otras personas.
- Se tiene muchas herramientas y sistemas para poder hacer el análisis y atender gestiones.
- Por temas de tiempo y carga laboral, muchas alertas se analizan y se descartan, pero nunca es igual que validarlas con el cliente.
- No hay un perfil de cliente con la información de él, ya que la misma se debe de formar en el momento de la alerta.
- La contactación es difícil, ya que los clientes no contesten para que confirmen la transacción
- La responsabilidad es 100% de los analistas.

9. ¿Qué propuestas y recomendaciones podría usted dar para una herramienta integradora de análisis y monitoreo de fraude?

   R. /

   - Seleccionar bien el proveedor si el desarrollo es externo, y si es interno, que los programadores tengan acompañamiento de especialistas de fraudes.
   - Que se tenga historial de transacciones y alertas mínimo de un año.
   - Que tenga incorporado las llamadas automáticas.
   - Que propongan mejoras a las reglas, considerando el falso positivo.
   - Que genere los patrones de fraudes, tanto por las alertas como las controversias.
   - Que se puedan marcar los fraudes masivos en módulos del core bancario.
   - Un sonido de las alertas.

- Que una parte del análisis lo realice la herramienta, conjugando todos los productos del cliente y su comportamiento.
- Que la herramienta vaya guardando patrones del análisis realizado por los analistas y que lo consideren en próximas alertas.
- Que se incorpore inteligencia de negocio y biometría.
- Que tenga datos de la interconexión financiera de central de riesgos.
- Las fuentes deben de ser siempre seguras y contar con garantías de seguridad de sistemas.

10. ¿Considera usted importante tener una herramienta integradora, donde se concentren los diferentes factores del proceso de monitoreo y prevención de fraude, así como la tecnología involucrada en inteligencia de negocio?

    R. / En su totalidad, los entrevistados consideran de suma importancia contar con una herramienta que una todas las actividades que están expuestas a un fraude, más ahora que la banca está buscando la digitalización de sus productos, toda organización debe de apostar e invertir no solo en la herramienta, sino en el recurso humano para ir previniendo las brechas que siempre se tendrán, porque aunque se tengan las herramientas más robustas se debe estar consciente que siempre hay un grado de riesgo.

    Hallazgos generales en la entrevista:

    - Se identificaron 11 herramientas de las cuales: 3 son motores de análisis, 2 son sistemas de información y 6 son complemento para poder desarrollar el trabajo.
    - Existen regulaciones y leyes que aplican para el proceso.

- Se generan 8 reportes que son requeridos para el análisis e información analítica.
- Se detectaron 13 elementos que debe de tener toda herramienta de análisis.
- El personal que gestiona las alertas, debe de tener habilidades analíticas, manejo de datos avanzada y conocimiento en auditoria forense.
- Se obtuvieron 12 recomendaciones para la herramienta de parte de los entrevistados.
- Los entrevistados, en una forma contundente concuerdan que es necesario tener una sola herramienta
- Se identificaron un total de 20 datos mínimos requeridos para poder realizar un análisis de alertamientos.

4.2.2. Resultados de la observación

Se implementó la técnica de la observación al proceso de monitoreo y prevención de fraudes, ejecutado por los cinco analistas, esta actividad se programó para ejecutarse durante 5 días agendados en los diferentes turnos, el departamento labora en un horario de 24/7 durante todos los días del año.

Tabla 9. Actividades observadas.

Actividad	Herramienta	Periodicidad	Tiempo requerido	Supervisión
Alertamientos de transacciones en TD y TC en VISA	VRM	Diario	Tuvo una duración promedio de 4 minutos y 09 segundos en cada caso.	No requiere de supervisión al momento del monitoreo, pero el jefe del departamento de monitoreo y prevención de fraude se encarga de validar el correcto abordaje de las mismas de manera diaria.
Alertamientos de operaciones en APP	IUVIPROFILER	Diario	Tuvo una duración promedio de 5 minutos y 08 segundos en cada caso.	
Alertamientos de transacciones en TC MasterCard	EMS	Diario	Tuvo una duración promedio de 4 minutos y 07 segundos en cada caso.	

Continuidad de tabla

Métricas o Dashboard	ICBS SISCARD CCC EXCELL	Diario, específicamente en el turno de 12 am a 6 am.	3 horas	Si requiere de supervisión posterior a la ejecución.
Atención de gestiones	CCC	Diario	Se observó un caso de gestión por parte del cliente, el cual lo abordó en 3 minutos.	
Atención de alertas pendientes	SISCO OAD	Diario	2 minutos	

4.2.2.1.Alertamientos de transacciones en tarjetas de crédito y débito VISA y MasterCard.

Se analizan las alertas efectuadas por el uso de tarjetas de débito y crédito, en el caso de VISA y en el caso de MasterCard solamente tarjetas de crédito; ya sea por el uso de las mismas en comercios físicos o electrónicos que reflejen altos índices de fraude, como también, el uso de cajeros automáticos que no presenten índices de seguridad adecuados, entre otros.

Para el análisis de las alertas, el analista ingresa con su clave y usuario a la herramienta VRM o EMS respectivamente, observando en la bandeja de alertamientos las transacciones que requieren de su análisis, selecciona cada una de ellas para ejecutar las acciones que en su estudio él considere, si la transacción no es considerada falso positivo procede a realizar contactación vía teléfono, tomando información básica del cliente de los sistemas ICBS y SISCARD, al contactar al cliente, hace preguntas sobre la transacción y seguridad como por ejemplo, los beneficiarios de cuenta, fecha de corte de su tarjeta, entre otros. Si el cliente reconoce la transacción le da por verificada, si el cliente no reconoce la transacción, la marca como fraude y notifica al área de controversia vía formularios de Google. Si el cliente no llegase a contestar, se coloca en estatus pendiente y bloquea preventivamente la tarjeta.

Una vez validando lo anterior, el analista ingresa a la herramienta ICBS, con el fin de obtener la información del usuario, digitando el número de tarjeta de crédito o débito; luego de extraer el número telefónico, se procede a contactar al cliente a través de la herramienta CISCO, en el cual el analista luego de ingresar el número telefónico ingresa una clave personal. Dicho proceso de contactación, afecta el tiempo invertido a cada alerta, ya que depende del tiempo que tarde el cliente en contestar o la duración de la llamada.

El tiempo de ejecución por cada alerta fue tomado cronométricamente, por lo tanto, el promedio del mismo se obtuvo a través de la suma de minutos registrados de la muestra aleatoria, en consideración a la carga de turno de 100 transacciones observadas y dividiendo el resultado entre el número de analistas, en este caso son 5.

Los estatus que pueden quedar las alertas son las siguientes:

- Declinada: la alerta es declinada por falta de indicadores de fraude.
- Buena: en caso de que el cliente asegure que efectivamente la transacción fue realizada.
- Fraude: en caso de que la transacción cumpla con todos los indicadores de un fraude.
- Pendiente: en el caso de no localizar al cliente, se envía un mensaje comunicándole lo sucedido y se bloquea la tarjeta de manera temporal, hasta que él mismo se contacte con el banco o se haga presente.

4.2.2.2. Alertamientos de operaciones en APP.

Está orientado para los clientes, que dan uso a la aplicación móvil de Davivienda, en la cual tienen la oportunidad de realizar diferentes gestiones como ser:

- Transferencias a cuentas de diferentes instituciones bancarias.

- Pagos de servicios varios.
- Recargas a teléfonos celulares, entre otros.

El analista cuenta con clave y código de seguridad para acceder a la plataforma IUVIPROFILE, en el cual el cliente es representado con un código, éste se deberá descodificar a través de una función dentro de la misma herramienta, la cual generará el número de identidad del cliente que él mismo es el usuario para ingresar a la APP. Luego de obtener el usuario, el analista procedió a ingresarlo en la herramienta ICBS para obtener el nombre, identidad y demás información necesaria para la contactación del cliente y validar a través de preguntas de seguridad si la persona es dueña de la transacción. Una vez validando si la transacción fue realizada o no por el cliente, el analista regresa a la herramienta para categorizarla en pendiente, si no se logró la contactación con el mismo, o en caso contrario, si el cliente contestó la llamada y validó que efectivamente la transacción fue realizada por él, se procede a situar la transacción como aceptada por el cliente.

4.2.2.3. Métricas o tableros de mando

El analista ingresa a los diferentes sistemas o herramientas, accediendo a estos a través de su usuario y clave dependiendo el sistema que considera como los es: VRM, EMS, ICBS, CCC, SICARD, esta información es ejecutada en QRY o SQL y trasladada a Excel para poder ser procesada en los formatos que se presentan, los envíos se hacen por correos electrónicos y por formularios de Google.

Dichas actividades se realizan en el turno de 12 a 6 am intermitentemente, considerando que el flujo de alertas es menor en comparación a otros turnos. La actividad de generar métricas es intercalada sobre las alertas que se van generando. La información que se genere es remitida al jefe del área, para que pueda revisarla y analizarla de manera

que sirva para establecer estrategias oportunas en el día a día laboral.

Las métricas que se generan son:

- Dashboard Monitoreo y Fraude: requiere de 40 minutos para su ejecución.
- Reporte de pendientes (TDD/TDC/APP): se realiza en un promedio de 1 hora.
- Detalle de TRXS fraudulentas aprobadas: 30 minutos es el tiempo promedio que requiere.
- Control de falso positivo: requiere de 20 minutos de ejecución.
- Salvado de tarjetas TRXS aprobadas: requiere de 20 minutos de ejecución.

4.2.2.4. Atención de gestiones.

Tiene como fin atender las gestiones o solicitudes del cliente con relación al uso de sus productos, como ser: consultas de saldos pendientes, disponibles o límite de crédito de las tarjetas; consulta de movimientos, entre otras.

Para dicho proceso, el analista ingresa a la herramienta CCC, en la cual acceden a través de su usuario que le da acceso a la bandeja de gestiones pendientes de atender. Los servicios que se atienden son: bloqueo o desbloqueo de usuario de APP, bloqueos o desbloqueos de tarjetas de crédito y débito, confirmación de transacciones y parámetros de avisos de viaje. Estas gestiones son ingresadas por los canales de atención al cliente. El analista visualiza el detalle de la gestión, enfocándose en los comentarios de la misma y dependiendo de éstos, ingresa a las herramientas de motor de fraudes que son: VRM, IUVIPROFILER y EMS, al concluir las mismas, retorna a CCC para finalizar la gestión. La duración del proceso fue de 2 minutos en cada caso y se realiza diariamente de manera frecuente, ya que dichas gestiones deben ser atendidas inmediatamente.

De igual forma, cabe recalcar que la experiencia adquirida con el tiempo de los analistas es un factor importante, ya que la ejecución del proceso y el abordaje del mismo

se realiza con mayor rapidez, así como el ser detallista con cada proceso le otorga un valor agregado a cualquier actividad asignada.

4.2.2.5. Atención de alertas pendientes.

Se genera reporte de las alertas pendientes resultantes de las tres herramientas: VRM, IUVIPROFILER y EMS, dicha información la ingresa a una hoja de cálculo de Google que es compartida vía Drive, la cual se carga en los sistemas de llamadas automáticas para que inicie la contactación con los clientes, al contestar éste cae la indicación en pantalla al analista para su atención, quien visualiza la información de número de tarjera o usuario de APP, monto y detalle de la transacción, el analista realiza validación con el cliente a manera de confirmar si es él quien realizó la transacción. Dicho proceso se realiza diariamente por los analistas y tiene una duración promedio de 2 minutos en la atención.

4.3. Análisis de los resultados

4.3.1. Factores

Para esta variable se establecieron los indicadores de cantidad de herramientas que se utilizan, los parámetros y datos que las mismas tienen o deberían de tener, a través de la indagación en la entrevista a las preguntas uno (1), dos (2) y tres (3) como apoyo.

En la pregunta 1 se logra obtener las herramientas que se están utilizando, que son en total 11, de las cuales 3 son aplicaciones o motores de análisis, 2 son sistemas de información y 6 son complemento para poder desarrollar el trabajo.

Pregunta 2 se logra identificar, que en la industria actualmente no se cuenta con una herramienta que integre en su totalidad los motores de análisis de prevención de fraude y el perfilamiento de clientes como una sola aplicación para el análisis, a pesar de que unos contestaron que sí, no es lo que esta propuesta espera realizar, los expertos

también aportaron lo importante que es estar a la vanguardia de la tecnología emergente, dando el ejemplo de las tarjetas digitales.

Pregunta 3, se obtuvieron un total de 20 datos, que los expertos y analistas determinan como los mínimos requeridos para un análisis de transacciones fraudulentas.

Con la observación a los 5 analistas en sus diferentes actividades, se pudo constatar la diversidad de herramientas que utilizan y que al estar interactuando pueden ocasionar desconcentración, así como generar tiempo que se suma a la carga laboral del talento humano.

4.3.2. Requerimientos técnicos, regulatorios y políticas

En todo proceso y actividad financiera es importante que se tengan controles, los cuales pueden ser para medir eficiencias, así como para mitigar el riesgo, considerando el tema de investigación, a esta variable se asignaron los indicadores de políticas, normas, regulaciones y métricas o estadísticas, los cuales a través de las preguntas cuatro (4) y cinco (5) se realizó la indagación.

Pregunta 4, se logra identificar que existen políticas vinculadas al proceso, así como las normas que la CNBS señala y que de igual manera las que el Estado establece, conjugando entre sí para asegurar información de los clientes y generar en esto seguridad de sus datos; por otra parte, la organización cuenta con procesos para cada actividad.

En la pregunta 5, el área de monitoreo y prevención de fraude genera 8 reportes con datos estadísticos diarios para poder medir la eficiencia operativa del área y de las reglas, dos de éstas es compartida con el área de gestión integral de riesgos, los entrevistados indican la complejidad de la generación y conformación de los mismos, lo que nos permite denotar una oportunidad para la propuesta de esta investigación.

En la observación a la ejecución de cada actividad del proceso, existen estándares establecidos, sin embargo, los analistas se guían por un orden de actividades diferentes ya que no todos cuentan con la misma experiencia de apoyo en la agilidad de la ejecución del proceso, cada actividad tiene una supervisión, por lo general posterior a su ejecución.

4.3.3. Proceso de la gestión de la tecnología

Esta investigación determina lo vital que, es la experiencia de las personas en temas que llegan hacer tan complejos como lo es el fraude, debido a esto, se considera esta variable para obtener información que apoye a la propuesta, estableciendo los indicadores de aportes, criterio y detalles de factores o elementos, es por ello, que a través de las pregunta seis (6) y siete (7) se indagó.

Pregunta 6, nos da un resultado de 13 factores que debe de tener o contemplar una herramienta, sobre todo es importante asegurar que los sistemas sean de alta seguridad, que si se contrata un proveedor para desarrollar la herramienta se hace con estándares altos de seguridad, que tenga la experiencia en el mercado de medios de pagos a nivel mundial preferiblemente.

En la pregunta 7 se pudo obtener 22 prácticas y técnicas que a lo largo de la experiencia de los entrevistados han vivido y están convencidos que cualquier herramienta debe de tener, igual la mayoría de ellos recalcaron lo vital que la misma sea en línea, es decir que esté interactuando inmediatamente, así como también que sea fácil de comprender en un lenguaje común.

A través de la observación, se determinó que los analistas poseen conocimientos necesarios para la ejecución de las actividades del proceso, sin embargo, al momento de indagar a través de preguntas más puntuales y sobre temas referentes al proceso y contextos, no tenían un conocimiento completo de los mismos.

4.3.4. Herramienta integradora en el proceso de análisis y prevención de fraudes.

Para esta variable se considera conocer las causas de manera que sean las mejoras a considera en la propuesta, de igual manera escuchar las recomendaciones y opiniones que apoyen a la aplicabilidad, por ello los indicadores se centran en las causas y propuestas, los cuales se indagaron en la pregunta ocho (8), nueve (9) y diez (10)

Pregunta 8 esta pregunta se aplicó a los ejecutores del proceso interno, todos concluyen que el estar interactuando entre varias herramientas hacen que se asuman riesgos de tiempo, de igual manera el análisis no es tan profundo, y la cantidad de alertas llevan muchas veces a descartar para confirmación y esto por la carga laboral, igual un problema que denotan los entrevistados externos es que la migración a canales digitales ha sido acelerada y eso ha expuesto a las organizaciones que a su vez en aras de atender necesidades de los clientes implementaron productos omitiendo la calidad y seguridad y eso es lo que está más aun afectando.

Pregunta 9 un total de 12 recomendaciones todas muy innovadoras desde algunas muy complejas hasta sencillas todas de manera de generar a los usuarios y clientes seguridad y simplicidad sin dejar de ver el riego del fraude.

En la pregunta 10 podemos determinar lo contundente que los entrevistados fueron en afirmar lo importante que es una herramienta que logue integrar los elementos y demás factores del proceso para mejorar la administración de la alertas y sobre todo que permita un análisis previo, durante y posterior de fraudes.

En la observación se denota que pese que las herramientas constatan con las necesidades para mitigar los riesgos, no se puede omitir que existen oportunidades de

mejora de manera de hacer aún más eficiente las actividades tanto en pro de la ejecución del analista, así como para la atención de los clientes.

4.4. Datos e información adicional recopilados

4.4.1. Política

Políticas de riesgo transaccionalidad para medios de pagos, tiene como objetivo establecer las normas y vigilancia a las transacciones que realizan los clientes bajo los niveles de riesgos estableciendo para ellos reglas que determinen la potencialidad de un fraude, su alcance es a todas las transacciones que se realicen en los diferentes canales que el banco ofrece, cuenta con un comité que mensualmente se reúne para analizar los sucesos y potencializar los riesgos operativos de manera de actuar o gestionar mejoras a la instrucciones que la política deriva.

Se observó que la política esta detallada y nombra responsabilidades por puestos y áreas las cuales instruyen controles de ejecución y seguimiento como también procesos, por lo que esta investigación los considera óptimos de cara a mitigar los riesgos de fraudes.

4.4.2. Reglas de alertamientos

Según la política el área de gestión integral de riesgo es la encargada de emanar las reglas para cada motor de análisis como lo son VRM, EMS y IUVIPROFAILE, las cuales se establece con un marcador de riesgo tolerable; estas deben ser revisadas de acuerdo su efectividad y en consideración con los casos materializados, el análisis se realiza en conjunto con las áreas de operaciones en tarjetas y negocios de medios de pagos ya que según política se deben sumar esfuerzo de cara a la continuidad del negocio, a nivel de productos de tarjeta de crédito y débito se tienen 17 reglas de declinación y 20

de alertamientos tanto para VRM y EMS, en cuanto la transaccionalidad en APP 16 reglas de declinación y 10 de alertamientos.

La reglas son los controles sin embargo estas no pueden permanecer estables ya que los fraudes son variables y el modo que operan los defraudadores evoluciona día a día por los nuevos elementos que se integran como lo es la tecnología y productos digitales.

4.4.3. Métricas

Se obtuvieron datos de las mismas en cada canal y herramientas, así como los análisis que se realizan de manera de establecer estrategias encaminadas a la eficiencia tanto en la parte de reglas, prevención y carga laboral, ésta información no se puede detallar en el presente informe debido a que es altamente restringida.

La información permitió conocer los días y horas de mayor demanda a niveles de las acciones de alertamientos de igual manera datos del contexto del proceso que apoyan a la investigación.

4.4.4. Encuestas satisfacción cliente

Se proporcionó a la investigación informe de encuesta que se realizado a los clientes para conocer su experiencia en cuanto a la contratación para la confirmación de las alertas de fraude en donde en su mayoría afirmaron estar satisfechos e indicando como una experiencia positiva y única que da seguridad a ellos, la satisfacción general es del 8.2% en una escala de 10%.

La contratación no se puede de obviar aun lo que se debe de hacer es buscar mejores mecanismo siempre cuidando la experiencia del cliente.

4.4.5. Estudio fuerza de trabajo

Para el mes de septiembre 2021 a solicitud de la gerencia de operaciones en tarjetas, el área de transformación del negocio apoyo para realizar análisis de la fuerza de trabajo de los analistas de monitoreo y prevención de fraude, esto como estrategia derivada del análisis de la cantidad de transacciones y alertas que abordan.

El alcance del estudio comprendió en aplicar un instrumento de recolección de datos para cada funcionario en un periodo de un mes, la medición se realizó considerando la fuerza de trabajo por empleado (FTE) y las dimensiones de evaluación comprendidas entre 0.8 -1.20 como normal, 1.21 – 1.40 limitado y 1.41 – 3.00 critico, lo 4 analistas dieron resultados de estar en un FTE crítico y 1 de ellos en limitada, el estudio también indica que existen actividades realizadas por el analista que dio resultado de limitada que no se pueden cuantificar en tiempo como lo es los análisis de casos materializados y actividades asignadas por el jefe.

La investigación al analizar el presente estudio considero oportuno sumar esfuerzo para que la propuesta contemplara medidas que apoyen al equilibrio de la carga laboral.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. En la presente investigación se confirmaron y se detallaron los diferentes factores actuales que influyen en el proceso de monitoreo y prevención de fraude, mismos que son considerados por los analistas y personas involucradas en el proceso, de igual forma se identifican algunos que las herramientas actuales no tienen, dando oportunidades para ser incluidos, todo esto conlleva un panorama más amplio para la propuesta que deberá de afirmar la seguridad y agilidad en las actividades, convirtiéndose en los beneficios que apoyen a los efectos identificados.
2. Existen regulaciones emanadas por la CNBS y leyes que el estado de Honduras ha generado, en donde alguno artículos específicos repercutan en la ejecución del proceso de monitoreo y prevención de fraude, de igual forma a lo interno Davivienda tiene establecido una apolítica que genera las directrices necesarias en el establecimiento de las reglas de alertamientos transaccional, sin embargo se pudo constatar que algunas de las personas involucradas en el proceso no las conocen a profundidad, lo que podría presentar problemática al momento de los análisis, para esta investigación fue de importancia establecer estos elementos para ser considerado en la propuesta.
3. A través de la investigación se demostró que el proceso de monitoreo y prevención de fraude contiene ciertas debilidades o aspectos que podrían ser reforzados o mejorados entre algunas; la contratación de los clientes, evaluación oportuna de eficiencia de las alertas y múltiples herramientas para el análisis. Con esto podemos indicar que por medio de la tecnología

emergente y la innovación se puedo obtener aportes sustanciales que apoyaron esta propuesta.

4. Esta investigación obtuvo de los involucrados en el procesos de monitoreo y prevención de fraude, así como expertos nacionales e internacionales conocedores de fraudes y de sistemas medios de pagos, un detalles de componentes, elementos y directrices que se deben de considerar al diseñar un prototipo de una herramienta integradora de análisis de transacciones fraudulentas, los expertos indicaron cuan importantes es que toda organización invierta en desarrollos para este tipo de sistemas.

5.2. Recomendaciones

1. Fortalecer los factores con los que actualmente cuenta Banco Davivienda, así como también considerar la oportunidad de incluir los factores que las herramientas no contemplan, de esta manera, el análisis que se requiere en las alertas del proceso de monitoreo y prevención de fraudes será ejecutado de manera más eficiente y ágil reduciendo tiempos y maximizando calidad en el servicio.
2. Reforzar bajo el proceso de comunicación interna periódicamente las políticas, normas y leyes establecidas para asegurar y certificar que a las personas involucradas en el proceso tengan el completo entendimiento y comprensión de las mismas, de manera de influir en el análisis de las actividades del proceso de monitoreo y prevención de fraude; estas normas, leyes y políticas deben de ser contempladas en las herramientas, así como en el proceso que la institución considere.
3. Considerar las oportunidades de mejora identificadas en esta investigación para eficientizar el proceso de monitoreo y prevención de fraude, así como

oportuno analizar las nuevas tendencias tecnológicas e innovadoras que puedan ser integradas para el análisis de alertamientos. Para que esta manera, puedan contaran con los beneficios ofrecidos por la misma posicionándose a la vanguardia de los avances tecnológicos y sobre todo reforzando la seguridad ante los fraudes.

4. Desarrollar una herramienta integradora para el proceso de análisis y prevención de fraudes que incluya los componentes y elementos necesarios para la ejecución del mismo, tomando en cuenta el diseño en versión de prototipo que se proporciona, asegurando mejorar las oportunidades identificadas en la indagación.

CAPÍTULO VI. APLICABILIDAD

Reseña histórica

Banco Davivienda Hondura es un ejemplo de la evolución y solides en el sistema financiero nacional a pesar que esta denominación social la adquiere en el año 2012 no se puede dejar de considerar la transcendencia de un grupo financiero de capital hondureños que en el años 1921 nace con la compañía de seguro el ahorro hondureño en donde después de años de estar en el mercado sus propietaria la señora Rosa Rivera de Smith vio la necesidad de crear en 1947 el banco la capitalizadora hondureña (BANCAHSA) el cual tenía el objetivo de ampliar su protocolo de servicios y así se fueron incorporando empresas como banco el ahorro hondureño (BANCAHORRO) , crédito hondureños (HONDUCARD) las cuales para el año 2000 se fusionaron conformando lo que se llamaría Banco Grupo El Ahorro Hondureños (BGA).

Para el año 2003 BGA es vendida a Banco del Istmo (Banistmo), que en un corto tiempo para el año 2006 se ve en la necesidad de aceptar oferta de Hong Kong and Shanghai Banking Corporation Limited (HSBC) en donde se posiciona en el quinto lugar del sistema financiero para el año 2012 HSBC vende sus acciones a el Grupo Bolívar tomado su nombre comercial de Banco Davivienda. (Davivienda, 2021)

En agosto de 1972 nace en Colombia la corporación colombiana de ahorro y vivienda con el nombre de Coldeahorro, la empresa inicio operaciones con un capital autorizado de 60 millones de pesos, y la “casita roja” como símbolo vigente hasta la fecha. Sin embargo, no es hasta en 1997 donde se convierte en banco comercial con el nombre de Banco Davivienda S.A. A partir de este momento el Banco Davivienda se enfoca en su consolidación en el sector financiero colombiano y la región. (Grupo Bolívar, 2021).

Misión y Visión

"Misión: Generar Valor para nuestros accionistas, clientes, colaboradores y terceros relacionados, apoyados en las siguientes destrezas:

- Conocimiento del Cliente
- Manejo del Riesgo
- Tecnología y Procesos
- Innovación
- Sinergia Empresarial
- Conocimiento del Negocio
- Manejo Emocional de las relaciones" (Davivienda, 2018d).

"Visión: Somos un conjunto de empresas privadas, sólidas y rentables. Compartimos una misma cultura corporativa y los mismos principios y valores corporativos" (Davivienda, 2021).

Canales y productos digitales

Davivienda Honduras cuenta con un portafolio amplio de productos y servicios entre los que podemos listar:

- Cuentas de ahorro con las características de las necesidades de las personas, dentro de las principales mencionamos, inversión, Pago de planilla y Multiahorro de remesas dando la facilidad de hacer uso de cajeros ATM y tarjetas de débitos contando con la posibilidad de apertura de cuentas en línea.
- Cuentas de cheques que son utilizadas tanto por personas jurídicas y naturales, con la generalidad uso de chequeras personalizadas.

- Dabuenavida y Depositos a plazo que consisten en depósitos fijos con un y ahorro programados.
- Otorgamientos préstamos para compra de vivienda, consumos, compra de auto e inversión para capital de trabajo tanto industrial y agro.
- Tarjeta de crédito bajo el licenciamiento de las marcas VISA y MasterCard con productos Clásica, Oro, Platinum, Empresarial, Corporativo, Black, Infinite y Signature que a su vez da la facilidades de intra y extra-financiamiento.

Entre otros productos y servicios que ofrece Davivienda: pago de remesas, garantías bancarias, transferencias internacionales, fideicomisos, pago de planillas, pago de servicios públicos y privados y emisión de cheques de caja. Todos estos productos y servicios están disponible para ser usado por los cliente tanto en banca en internet como en APP más todas las sucursales y oficinas del banco.

Davivienda tiene 42 agencias y 76 cajeros automáticos (ATM sus siglas en inglés) ubicados en 12 departamentos del territorio nacional distribuidas de la siguiente manera: Cortes 12, Francisco Morazán 11, Atlántida 4, Yoro 3, Islas de la Bahía 2, Colón 2, Olancho 2, Comayagua 2, Nacaome 1, Copan 1, Choluteca 1, El paraíso, 1.

Figura 3. Localización y funcionalidad de los ATM.

Fuente: (Davivienda , 2021)

DAVIVIENDA

MOTOR INTEGRADO DE FRAUDE DE DAVIVIENDA

ÍNDICE

6.1. Nombre de la propuesta

"MOTOR INTEGRADO DE FRAUDE DE DAVIVIENDA"

Fuente: Lasrozas

6.2. Justificación de la propuesta

Con este diseño de propuesta, se espera que Banco Davivienda pueda tener un horizonte de los requerimientos mínimos para contar con una herramientas integradora para el análisis de fraudes, pretendiendo así abarcar las oportunidades de mejora que a través de esta investigación se pudieron identificar, basadas en hacer más ágil el proceso a través de una forma innovadora, atributos que el banco comparte en su filosofía organizacional.

Este diseño del motor integrador de fraude de Davivienda comprenderá: factores identificados como prioritarios para el análisis de alertas, que se mostrará en forma de un perfil de clientes, se asegura el cumplimiento de las regulaciones, normas y leyes que en esta investigación se detectaron, eficientar los tiempos de contactación y de ejecución que apoyarían la disminución de carga laboral y reclamos de los clientes de igual manera, se consideraron patrones de análisis que, a través de la indagación con expertos se

identificaron, logrando así cerrar brechas que han o pueden concluir en el registro de riesgos operativos.

Este motor integrador traerá beneficios, que tienen como finalidad englobar las alertas y patrones de fraudes, que permitan actuar ante los ataques a los cuales el banco es expuesto a través de la transaccionalidades que sus clientes realizan en los canales digitales y comercios físicos.

6.3. Alcance de la propuesta

- Optimizar el proceso de monitoreo y prevención de fraude, utilizando el motor integrador, el cual permitirá la reducción de los tiempos de contactación del 20.5% en alertamientos de tarjetas de crédito y débito, un 23% para APP y en cuanto a generación de métricas un 100%, del asegurando un porcentaje de contactación y gestión del 98% mínimo.
- Agregar elementos que las herramientas actuales no contemplan ni pueden fácilmente adherirlos, estos fueron identificados en la observación del proceso, así como en la indagación de expertos y ejecutores, facilitando así el análisis como también la generación de un perfil de comportamiento del cliente.
- Proporcionar un documento de requisitos comerciales (BRD por sus siglas en inglés) al área de operaciones en tarjetas de Davivienda para que le sirva de guía en la solicitud de desarrollo de un motor integrador de fraude.
- Asegurar bajo esta herramienta el cumplimiento oportuno de las normas, leyes y regulaciones, específicamente los artículos vinculados al fraude, adhiriendo al motor integrador de fraude directrices y parámetros.
- Rentabilizar los recursos y sistemas de información que ya cuenta el banco, de manera de utilizar en la generación de esta herramienta que apoyara en la mitigación de fraude.

- Proponer medidas a corto plazo que apoyarán al proceso y generarán motivación al talento humano, a través de evaluación de las alertas de APP con una reducción del 81%, el trabajo colaborativo, capacitaciones y una evaluación de descripción de puestos.

6.4. Descripción y desarrollo a detalle de la propuesta.

6.4.1. Desarrollo de la propuesta.

DOCUMENTO DE REQUISITOS COMERCIALES

DAVIVIENDA

El área de operaciones en tarjetas con su unidad dependiente, como los es el departamento de monitoreo y prevención de fraude, son los encargados de parametrizar las alertas y a su vez de evaluarlas a través de un análisis que implica la confirmación con los clientes, que son usuarios de tarjetas de crédito, tarjetas de débitos y APP.

Figura 4. Registro de tiempo de ejecución en cada herramienta

Herramientas	Ingreso al sistema	Datos de colas de alertas	Conversor TODO1	Información en ICBS o Siscard	Contactación CISCO	Ingreso de observaciones	Marcación de status de alertas	Bloqueo en ICBS	Mensaje o correo informativo	Total de tiempo	Métricas
VISA	5 s	15s		20 s	3 min*	40 s	4 s	4 s	30 s	4.9 s	1 hora
mastercard	5 s	10 s		20 s	3 min*	30 s	4 s	4 s	30 s	4.7 s	1 hora
IUVIPROFILER	5 s	15 s	1 min		3 min*	45 s	4 s	4 s	35 s	5.8 s	1 hora

Fuente: creación propia.

El proceso de análisis y prevención de fraudes de Banco Davivienda reducirá tiempo en su ejecución ya que, como se muestra en la imagen anterior, 6 actividades sombreadas en color naranja, serán reducidas del proceso que actualmente los analistas cumplen, dando como resultado una reducción en los tiempos y un mayor inclusión en

las alertas de fraude, brindando un margen de riesgo menor al actual. Siendo de gran beneficio para el proceso actual.

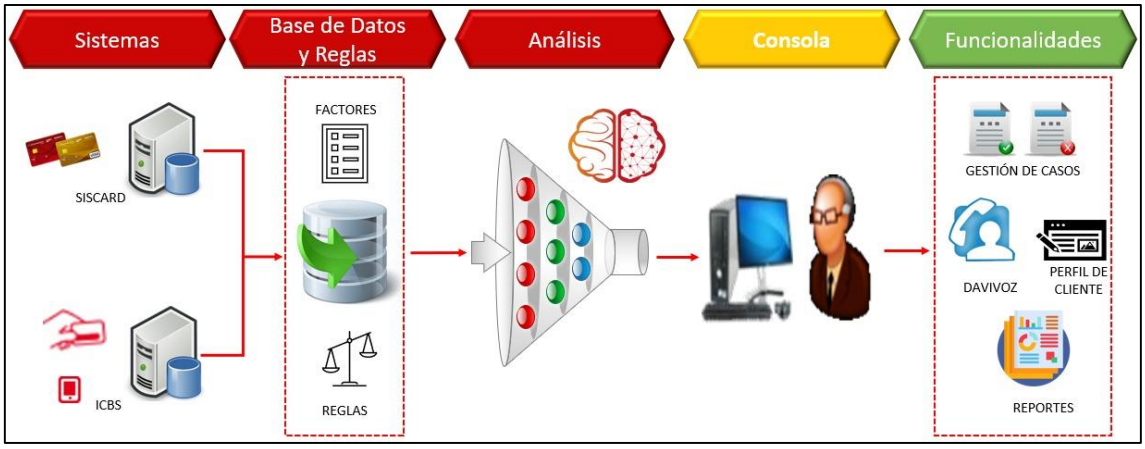
6.4.1.1. Detalle y generalidades de la propuesta

Esta consiste en desarrollar un programa en ICBS u otro sistema de información, la cual permitirá contar con un solo motor de análisis de fraude, que concentrará las alertas de transacciones fraudulentas derivadas de la transaccionalidad que los clientes realizan con sus tarjetas de débito, crédito y APP.

El motor integral de fraude deberá de considerar los elementos mínimos para un análisis, los cuales se concentrará en un solo archivo, que a su vez se han extraído de las diferentes bases de datos de donde se originan las transacciones, estos datos permitirán que la herramienta realice un análisis de acuerdo con las alertas y demás parámetros que se coloquen, esta información se mostrará para que el analista pueda gestionar cada caso de acuerdo con una clasificación y prioridad.

Entre las funcionalidades del motor se estiman que sean: apoyo en la confirmación de una forma automática para algunas alertas, facilidad en la generación de reportes, mostrar gráficos analíticos de la eficiencia laboral y de reglas.

Figura 5. Diseño de la propuesta "Motor Integrador de Fraude Davivienda"



Fuente: creación propia

6.4.1.2. Requerimientos Funcionales

Código	**Requerimiento funcional 1 (RF1)**		
Nombre	Función y perfiles de usuarios	**Tipo**	N
Prioridad	1	**Responsable**	Por definir
Detalle			

Se requiere que el acceso a la herramienta sea de acuerdo a un perfil de usuario y para ello se consideran 4:

a) Perfil del analista: este perfil deberá de tener acceso a las gestiones de cada caso únicamente podrá realizar mantenimientos que se considera como gestión de caso, así como la visualización de los estadísticos o métricas de eficiencia.
b) Perfil del Administrador: tendrá acceso a realizar mantenimiento a la cesión de parámetros de reglas, generación de reportes y todo lo vinculado a la gestión de casos, así como la visualización de gráficos de eficiencia, ideado para el jefe de monitoreo y gerente de operaciones en tarjetas.
c) Perfil de Consultas: este perfil podrá visualizar los casos pendientes de atender, los atendidos, histórico de gestiones, generar reportes y obtener gráficos de eficiencia.
d) Perfil de seguridad: este perfil tendrá la facultad de otorgar los permisos a los usuarios de acuerdo a los perfiles antes mencionados.

Cada usuario podrá ingresar con su correo institucional y una clave que será asignada al momento que se habilite el acceso, que podrá ser modificada por el usuario y permitirá reseteo de la misma según las normas de informática de la institución cada mes.

Figura 6. Pantalla de inicio.

Fuente: creación propia

El correo institucional debe ser validado a través de interface en tiempo real, de manera que ningún correo que no esté activo por la organización pueda acceder a la plataforma.

Código	**Requerimiento funcional 2 (RF2)**		
Nombre	Base de datos (Archivo)	**Tipo**	N
Prioridad	1	**Responsable**	Por definir

Detalle

Continuidad de formato

La plataforma debe de obtener en tiempo real, información de los sistemas de tarjeta de crédito SISCARD y del core bancario ICBS información de la tarjetas de débito, cuentas, movimientos de éstas, datos generales del cliente, la que se concentra en un solo archivo que almacenará la información en una forma histórica, en cuanto al historial se deberá de considerar para temas de ICBS el archivo TA05010 de la biblioteca BNKPRD01 y en SISCARD el archivo MASTAJ03 de la biblioteca SICARLINE.

La clave de estos datos será el número de cliente asignado por el banco y el número de tarjeta de identidad.

Los datos que deberá de contener son los siguientes:

No.	Campo	Sistema	Archivo	Tipo de Campo	Longitud
1	Número cliente	ICBS y SISCARD	CUP01 / MaeTarj	Numérico	9 dígitos
2	Identidad	ICBS y SISCARD	CUP01/ MaeTarj	Numérico	13 dígitos
3	Nombre del cliente	ICBS	CUP01	Alfanumérico	N/A
4	Celular	ICBS	CUP01	Numérico	8 dígitos
5	Email	ICBS	CUP02	Alfanumérico	N/A
6	Tipo de ingreso	ICBS	CUP03	Número	N/A
7	Ciudad	ICBS	CUP04	Alfanumérico	N/A
8	Empleador	ICBS	CUP05	Alfanumérico	N/A
9	Perfil de riesgo	ICBS	CR01_Ri	Alfanumérico	N/A
10	Número tarjeta	SISCARD	MaeTarj	Número	16 dígitos
11	Tipo de tarjeta	Se deberá de generar considerando el código de producto *			
12	Saldo actual	SISCARD	MaeTarj	Número	N/A
13	Estatus_TDC	SISCARD	MaeTarj	Alfanumérico	N/A
14	Financiamiento	SISCARD	MaeTarj	Número	N/A
15	Monto financiamiento	SISCARD	MaeTarj	Número	N/A
16	Estatus	SISCARD	MaeTarj	Número	N/A
17	Número de débito	ICBS	BantTDB	Número	16 dígitos
18	Estatus tarjeta	ICBS	BantTDB	Alfanumérico	N/A
19	Fecha activación	ICBS	BantTDB	Numérico	DD/MM/AA
20	Fecha punto de reorden	ICBS	BantTDB	Alfanumérico	N/A
21	Agencia	ICBS	BantTDB	Alfanumérico	N/A
22	Número de cuenta	ICBS	Tap002	Numérico	13 dígitos
23	Estatus cuenta	ICBS	Tap002	Numérico	N/A
24	Tipo de cuenta	ICBS	Tap002	Numérico	N/A
25	Tipo producto	ICBS	Tap002	Numérico	N/A
26	Saldo	ICBS	Tap002	Numérico	N/A

27	Número de préstamo	ICBS	LNP00301	Numérico	N/A
28	Nombre del producto	ICBS	LNP00301	Numérico	N/A
29	Fecha desembolso	ICBS	LNP00301	Numérico	DD/MM/AA
30	Estatus mora	ICBS	LNP00301	Numérico	N/A
31	Saldo actual	ICBS	LNP00301	Numérico	N/A
32	Usuario APP	ICBS	APP_DavHn	Numérico	13 dígitos
33	Estatus2	ICBS	APP_DavHn	Alfanumérico	N/A
34	Fecha_app	ICBS	APP_DavHn	Numérico	DD/MM/AA
35	Fecha_OTR_TDC	SISCARD	MaeTarj	Numérico	DD/MM/AA
36	Saldo_TDC	SISCARD	MaeTarj	Numérico	N/A
37	Fecha_extra	SISCARD	MaeTarj	Numérico	DD/MM/AA
38	Método	ICBS	APP_DavHn	Alfanumérico	N/A
39	Controversia	ICBS	Mod_Conrtro	Numérico	N/A
40	Cargo recurrente	SISCARD	MaeTarj	Alfanumérico	N/A
41	Velocidad transaccional	ICBS y SISCARD	TAP0201 / MaeTarj	Numérico	00:00:00
42	Fecha de Nacimiento	ICBS	CUP02	Numérico	N/A
43	Dirección de casa	ICBS	CUP02	Alfanumérico	N/A
44	Número de casa	ICBS	CUP02	Numérico	8 dígitos
45	Posición	ICBS	CUP02	Alfanumérico	N/A
46	Dirección de empleo	ICBS	CUP02	Alfanumérico	N/A
47	Número de trabajo	ICBS	CUP02	Numérico	8 dígitos
48	Relacionados	ICBS	CUP02	Alfanumérico	N/A
49	Dependientes	ICBS	CUP02	Alfanumérico	N/A
50	Nacionalidades	ICBS	CUP02	Alfanumérico	N/A
51	Actividad. C	ICBS	CUP02	Alfanumérico	N/A
52	Estado actualización	ICBS	CUP02	Alfanumérico	N/A
53	Riesgo	ICBS	CR01_Ri	Alfanumérico	N/A
54	Fecha actualización	ICBS	CUP02	Numérico	DD/MM/AA
55	Próxima actualización	ICBS	CUP02	Alfanumérico	DD/MM/AA
56	Canal última actualización	ICBS	CUP02	Alfanumérico	N/A
57	Cuentas firmante	ICBS	CUP02	Alfanumérico	N/A
58	Cargos públicos	ICBS	CUP02	Alfanumérico	N/A

Fuente: creación propia

*El tipo de tarjeta de crédito se determina con los 8 primeros dígitos de la tarjetas

Marca	Código BIN	Producto
Visa	41115200	Débito
	45682400	Crédito Clásica
	41523700	Crédito oro
	43034900	Empresarial
	43035000	Corporativa
	43034800	Crédito Platinum
	41119500	Crédito Infinite
	48824500	Crédito Signature
MasterCard	55585500	Crédito Clásica
	55585501	Crédito oro
	55585502	Crédito Platinum
	55585503	Blanck

Código	Requerimiento funcional 3 (RF3)		
Nombre	Parámetros y Reglas de análisis	**Tipo**	N
Prioridad	1	**Responsable**	Por definir
Detalle			

La plataforma debe de tener la bondad de una subfunción, que permita que un usuario con el perfil de administrador (jefe de monitoreo y gerente del área) pueda parametrizar las reglas, que según política deben de considerarse en el análisis del motor integral de fraude, así como también otros campos en cumplimiento a las regulaciones.

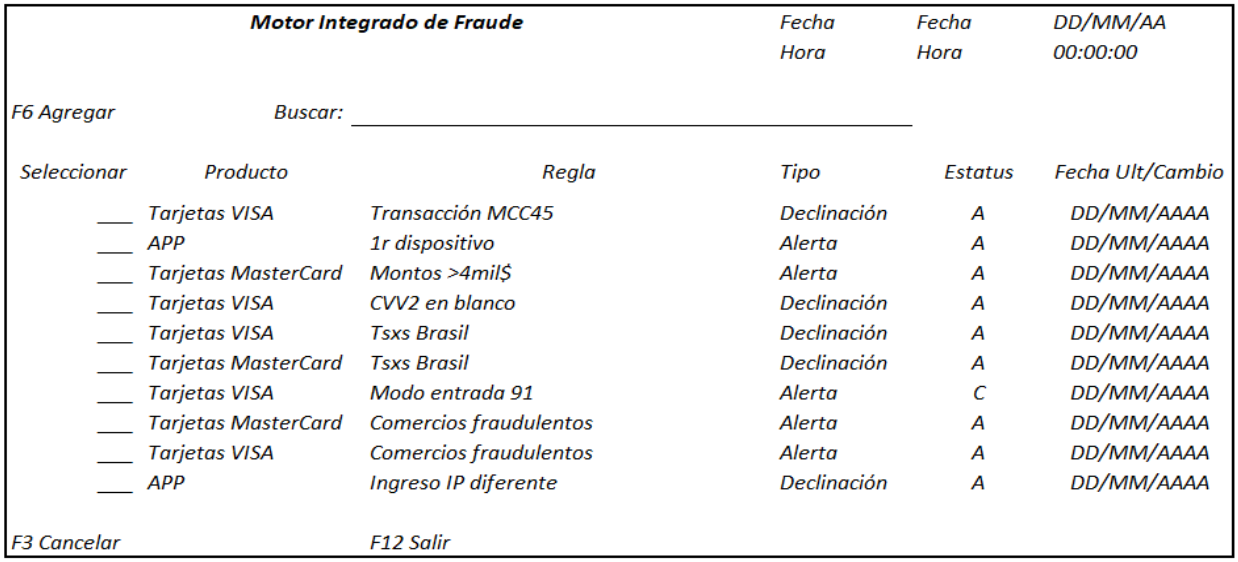
Figura 7. Pantalla de reglas y parámetros.

Fuente: creación propia

a) Reglas de monitoreo

Al seleccionar reglas de monitoreo, le mostrará una pantalla donde le permitirá: modificar, visualizar el listado de las existentes o agregar una nueva.

Figura 8. Consulta de reglas.



Motor Integrado de Fraude — Fecha DD/MM/AA — Hora 00:00:00

F6 Agregar — Buscar: _____

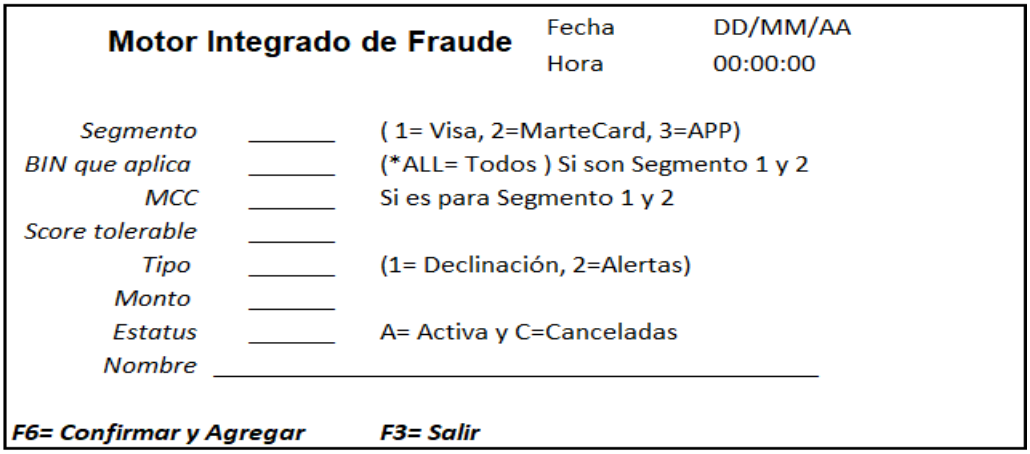
Seleccionar	Producto	Regla	Tipo	Estatus	Fecha Ult/Cambio
___	Tarjetas VISA	Transacción MCC45	Declinación	A	DD/MM/AAAA
___	APP	1r dispositivo	Alerta	A	DD/MM/AAAA
___	Tarjetas MasterCard	Montos >4mil$	Alerta	A	DD/MM/AAAA
___	Tarjetas VISA	CVV2 en blanco	Declinación	A	DD/MM/AAAA
___	Tarjetas VISA	Tsxs Brasil	Declinación	A	DD/MM/AAAA
___	Tarjetas MasterCard	Tsxs Brasil	Declinación	A	DD/MM/AAAA
___	Tarjetas VISA	Modo entrada 91	Alerta	C	DD/MM/AAAA
___	Tarjetas MasterCard	Comercios fraudulentos	Alerta	A	DD/MM/AAAA
___	Tarjetas VISA	Comercios fraudulentos	Alerta	A	DD/MM/AAAA
___	APP	Ingreso IP diferente	Declinación	A	DD/MM/AAAA

F3 Cancelar — F12 Salir

Fuente: creación propia

Si da el comando de F6 agregar una nueva alerta:

Figura 9. Incorporación y mantenimiento a reglas.



Motor Integrado de Fraude — Fecha DD/MM/AA — Hora 00:00:00

Segmento	_____	(1= Visa, 2=MarteCard, 3=APP)
BIN que aplica	_____	(*ALL= Todos) Si son Segmento 1 y 2
MCC	_____	Si es para Segmento 1 y 2
Score tolerable	_____	
Tipo	_____	(1= Declinación, 2=Alertas)
Monto	_____	
Estatus	_____	A= Activa y C=Canceladas
Nombre	_____	

F6= Confirmar y Agregar — **F3= Salir**

Fuente: creación propia

b) Parámetros regulatorios

En aras de cumplir la regulación y hacer una experiencia del cliente, se podrá incluir filtros que previo a una autorización sea de tarjetas o APP el motor delimita transaccionalidades apareciendo al usuario en la siguiente pantalla:

Figura 10. Parámetros de reglas.

Fuente: creación propia

Código	**Requerimiento funcional 4 (RF4)**		
Nombre	Análisis	**Tipo**	N
Prioridad	1	**Responsable**	Por definir
Detalle			

Al tener configurado la base concentradora, las reglas de monitoreo y parámetros, se deberá de realizar el análisis de las alertas las cuales se deberá de considerar lo siguiente:

a) Score de fraude: para este el motor debe de considerar el histórico de transaccionalidad, los tipos de comercios, tipo de transacción presente y no presente, histórico de transacciones del cliente y velocidad de la autorización. Dará como resultado un porcentaje, que es el que tomará la alerta ejemplo:

Tabla 10. Ejemplo de cálculos score.

Tipo de comercio	Tipo de transacción	Histórico en Comercio	Velocidad	Monto	Score
Supermercado	Presente	Si	00:00:01	100.00	0.8000
Hotel	Presente	No	00:00:01	2,500.00	0.6000
Hotel	No presente	Si	00:00:01	2,500.00	0.4000

Fuente: creación propia

b) Clasificación de prioridad: en una tabla se deberán de colocar los parámetros para cada factor, que determine por producto y tipo de transacción si la alerta procederá a llamar con alta prioridad o baja, así como, que la herramienta genere un auto confirmación con una llamada robótica.

Llamada: el analista deberá de llamar.

Gestionar: el analista deberá de hacer un análisis y determinar si es falso positivo

Auto gestión: será realizada por autenticación del cliente en una llamada robótica.

Llama Gestiona Auto gestión

Ejemplo de tabla:

Figura 11. Análisis de prioridad.

Factores	Llamar		Gestionar		Auto gestión	
Producto (VISA. MasterCard y APP)	VISA	APP	MasterCard	MasterCard	APP	VISA
Tipo de tarjetas (Si aplica)	Oro	N/A	Black	Clásica	N/A	Debito
BIN (Si son Tarjetas)	415237	N/A	55585503	55585500	N/A	411152
Apertura de Cta.	N/A	<3 días	N/A	<3 días	<10 días	N/A
Tipo de transacción	Presente	Traslado	Presente	No presente	Traslado	Presente
Comercio fraudulento	Si	N/A	Si	Si	N/A	N/A
Monto	>$20	> L. 100,000	>$20	> L. 2,500	> L. 5,000	> L. 1,000
Score de transacción	<0.300	< 0.300	<0.300	> 0.900	< 0.300	< 0.100
Perfil de riesgo del Cliente	Alto	Alto	Alto	Medio	Bajo	Bajo
Actualización de datos personales	<3 meses	<3 meses	<3 meses	<3 meses	<3 meses	N/A
Falso positivos anterior	Si	No	Si	No	No	Si
Saldo disponible	>50% del límite	>L. 500,000	>50% del límite	>50% del límite	> L. 1,000	> L. 1,000

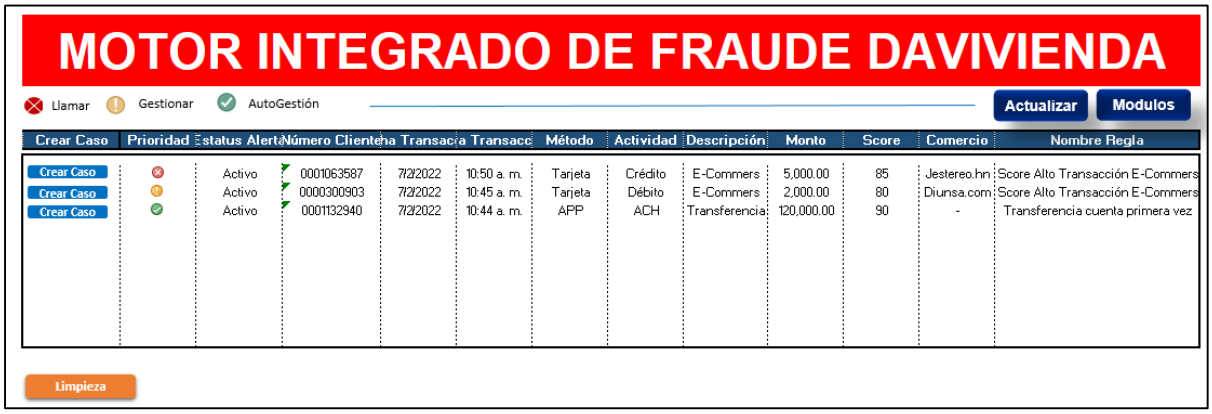
Fuente: creación propia

Código	Requerimiento funcional 5 (RF6)		
Nombre	Consola de gestión	**Tipo**	N
Prioridad	1	**Responsable**	Por definir
Detalle			

Considerando el análisis al usuario que trabajará las alertas, le deberá de aparecer una bandeja de entradas de las mismas, esta funcionalidad solo será disponible para el perfil de analista, ésta se espera se muestre de la siguiente manera.

La consola mostrará los datos de la transacción a confirmar, sea de tarjeta de crédito y débito, como APP que al igual deberá de contar con un botón denominado “Crear caso” que llevará al usuario al perfil del cliente.

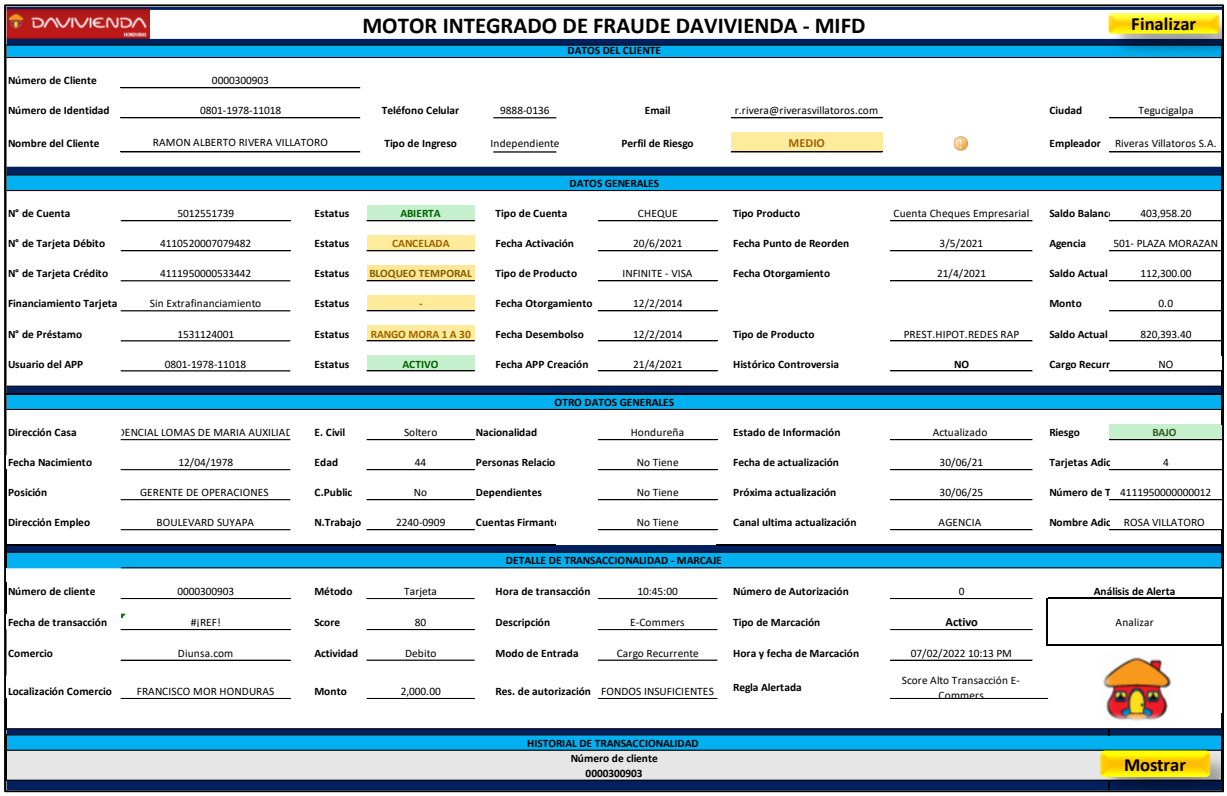
Figura 12. Bandeja de alertas.



Fuente: creación propia

Al seleccionar “crear caso” deberá de presentarse los elementos y factores para el análisis de la siguiente manera:

Figura 13. Perfil del cliente.



Fuente: creación propia

Deberá de tener la bondad de enlazar la llamada con el cliente, considerando el número de celular del mismo y un intento de 2 veces de contactación, en caso de no, se finalizará colocando en estatus de pendiente y generar un mensaje y correo de texto al cliente, indicando que debido a su seguridad su producto ha sido bloqueado y que deberá de contactar al banco, de igual manera caerá el caso en una bandeja de seguimiento, para que al término de atención de casos se pueda retomar la contactación por el analista o bien derivar a una DAVIVOZ.

Al finalizar el caso el analista, debe de colocar comentario de su gestión, así como un estatus en el que queda clasificada el mismo, los cuales podrán ser: descartada, fraude, buena y pendiente. Estos datos deberán de ser almacenados en el archivo y en el caso de que es fraude, conllevara a una cancelación o bloqueo del producto y si es pendiente, bloquear el producto generando mensajes y correos dirigidos al cliente o bien una DAVIVOZ.

Mantenimientos

En caso de una confirmación posterior, el analista podrá retomar el caso e indicar sus comentarios colocando si la transacción es descartada, de fraude o buena, tomando el flujo que competa y dejando en el archivo la fecha que se confirmó.

Si por algún motivo existiera una equivocación en el manejo del caso, este se apertura pidiendo una justificación la cual al terminar los cambios será identificada en el archivo histórico, de manera que pueda ser fácilmente identificada, como medida de seguridad del sistema no podrá realizar más de un intento por cada caso.

Código	**Requerimiento funcional 6 (RF6)**		
Nombre	Llamada DAVIVOZ Mensaje y correo	**Tipo**	N
Prioridad	2	**Responsable**	Por Definir
Detalle			

a) Llamada DAVIVOZ, esta funcionalidad tendrá que considerar las herramientas de llamadas, para que bajo un mensaje pregrabado y considerando los detalles de la transacción a confirmar llame al cliente, el cual en una confirmación de respuesta podrá indicar si realizó la operación.

La nota deberá de indicar así:

Para tarjeta de crédito y Debito

Buenos días/Tarde / Noche Sr o Sra. (Nombre), Banco Davivienda desea confirmar la transacción realizada por su persona por la cantidad de L. (Monto), con su tarjeta (crédito o débito), terminación en el comercio (nombre del comercio), el día 27 noviembre 2021, si es así, favor confirmar marcando **1,** si no es así, marcar **2,** y si desea escuchar el mensaje nuevamente

marcar **3** o Colgar para finalizar la llamada.

Para transacciones APP

Buenos días/Tarde / Noche Sr o Sra. (Nombre), Banco Davivienda desea confirmar la transacción realizada por su persona por la cantidad de L. (Monto), a través de nuestro canal digital APP, el día 27 noviembre 2021, si es así favor confirmar marcando **1,** si no es así, marcar **2,** y si desea escuchar el mensaje nuevamente marcar **3** o colgar para para finalizar la llamada.

b) Mensajes de texto y correo electrónicos

Se deberá de adicionar a los mensajes que se remiten, un link para que el cliente pueda en el caso de que sea una transacción de tarjeta de débito o crédito, realizar la confirmación por su APP o bien, que lo enlace al chat de la web del banco para que confirme la transacción.

Si fuera por transacciones de APP, únicamente deberá de direccionarlo a un chat de la web del banco.

Código	**Requerimiento funcional 7 (RF7)**		
Nombre	Reportes y Gráficos	**Tipo**	N
Prioridad		**Responsable**	
Detalle			

a) Reportes

Se requiere una sub función que permita extraer los siguientes reportes:

1. Reporte de casos pendientes: para este se debe de considerar el estatus pendiente de las transacciones que no se han podido confirmar.
2. Detalle de transacciones fraudulentas confirmadas: se considera el estatus fraude en

las transacciones.

3. Reporte de falso positivo: se considerarán los casos con estatus descartado.
4. Salvado de transacciones aprobadas: se tomará el monto de la transacción que se confirma como no fraude.

Todos estos reportes deberán ser parametrizables con:

- Fecha de transacción
- Fecha de contactación
- Hora de transacción y contactación
- Monto
- Detalles básicos de la transacción
- Alerta que la denotó
- Prioridad de Contactación
- Usuario que gestionó el caso

Ejemplo del reporte

Figura 14.Reporte para análisis.

No.	Fecha de transacción	Hora de transacción	Fecha de contactación	Hora de contactación	Tarjeta /Cta.	Producto	Monto Transacción	Perfil de Riesgo	Código de Alerta	Monto Salvado LPS	Monto Salvado $	Prioridad de Contactación	Usuario que gestionó
1	1/11/2021				4.11052E+15	TDD				0	0		
2	1/11/2021				4.11052E+15	TDD				91.42	3.66		
3	1/11/2021				4.11052E+15	TDD				1172665.1	46906.6		
4	1/11/2021				4.11052E+15	TDD				0	0		
5	1/11/2021				4.11052E+15	TDD				0	0		
6	1/11/2021				4.11052E+15	PP				96.56	3.86		
7	1/11/2021				4.11052E+15	TDD				0	0		
8	1/11/2021				4.11052E+15	TDD				0	0		
9	1/11/2021				4.11052E+15	TDD				38830.12	1553.2		
10	1/11/2021				4.11052E+15	APP				1689.98	67.6		
11	1/11/2021				4.30348E+15	TDC				249900	9996		
12	1/11/2021				4.30348E+15	TDC				76076.56	3043.06		
13	1/11/2021				4.30348E+15	TDC				0	0		
14	1/11/2021				4.56824E+15	TDC				35117	1404.68		
15	1/11/2021				4.56824E+15	TDC				238.68	9.55		
16	1/11/2021				4.56824E+15	TDC				1626.65	65.07		
17	2/11/2021				4.11052E+15	TDD				40	1.6		
18	2/11/2021				4.11052E+15	TDD				658.35	26.33		
19	2/11/2021				4.11052E+15	TDD				22.03	0.88		
20	2/11/2021				4.11052E+15	TDD				5238.58	209.54		

Fuente: creación propia

b) Tablero de mandos **(DASHBOARD)**

Bajo filtros, deberá de concentrarse lo que se requiere en el tablero de mandos necesarios para la evaluación de las estrategias, tomar la marca, el tipo de producto, estatus del caso, cantidades de transacciones, montos y calcular los porcentajes de contacto positivo, en donde éste es el monto confirmado entre el total de alertamientos, de igual manera, calcular el porcentaje de declinaciones, que resulta de dividir el total de transacciones declinadas entre el total aprobadas.

Figura 15. Dashboard.

Descripción	22-nov	23-nov	24-nov	25-nov	26-nov	Acumulado del Mes
Total VISA	**437**	**355**	**422**	**503**	**612**	**14,007**
Tarjeta de Crédito	193	160	211	236	294	4696
Tarjeta de Débito	244	195	211	267	318	9311
Descartada	282	197	286	310	328	6056
Fraude	57	68	55	67	94	5696
Buena	89	70	55	75	70	1814
Pendientes	9	20	26	51	56	377
% Contacto Positivo	**96.50%**	**96.70%**	**96.80%**	**96.90%**	**96.30%**	**96.26%**
Total Autorización VISA	**18,709**	**19,583**	**19,930**	**20,472**	**20,472**	**500,452**
Cantidad de Aprobaciones	15,719	16,414	16,973	17,101	17,101	411,899
Cantidad de Declinaciones	2,990	3,169	2,957	3,371	3,371	88,553
% de Aprobación	**84.00%**	**83.80%**	**85.20%**	**83.50%**	**83.50%**	**82.30%**
% de Declinación	**16.00%**	**16.20%**	**14.80%**	**16.50%**	**16.50%**	**17.70%**
Total MASTERCARD	**0**	**0**	**0**	**0**	**0**	**4**
Tarjeta de Crédito	0	0	0	0	0	4
Descartada	0	0	0	0	0	0
Fraude	0	0	0	0	0	0
Buena	0	0	0	0	0	4
Pendientes	0	0	0	0	0	0
% Contacto Positivo	**0.00%**	**0.00%**	**0.00%**	**0.00%**	**0.00%**	**100%**
Total Autorización MASTERCAR	**18709**	**19583**	**19930**	**20472**	**20472**	**500452**
Cantidad de Aprobaciones	15,719	16,414	16,973	17,101	17,101	411,899
Cantidad de Declinaciones	2,990	3,169	2,957	3,371	3,371	88,553
% de Aprobación	**84.00%**	**83.80%**	**85.20%**	**83.50%**	**83.50%**	**82.30%**
% de Declinación	**16.00%**	**16.20%**	**14.80%**	**16.50%**	**16.50%**	**17.70%**
Total APP	**106**	**97**	**91**	**96**	**95**	**2744**
Buena	36	16	17	9	1	829
Fraude	0	0	0	0	0	19
Descartada	41	51	28	40	49	1617
Total Pendientes	29	30	46	47	48	266
Monitoreo	29	30	46	47	48	266
No aparece el usuario	0	0	0	0	0	0

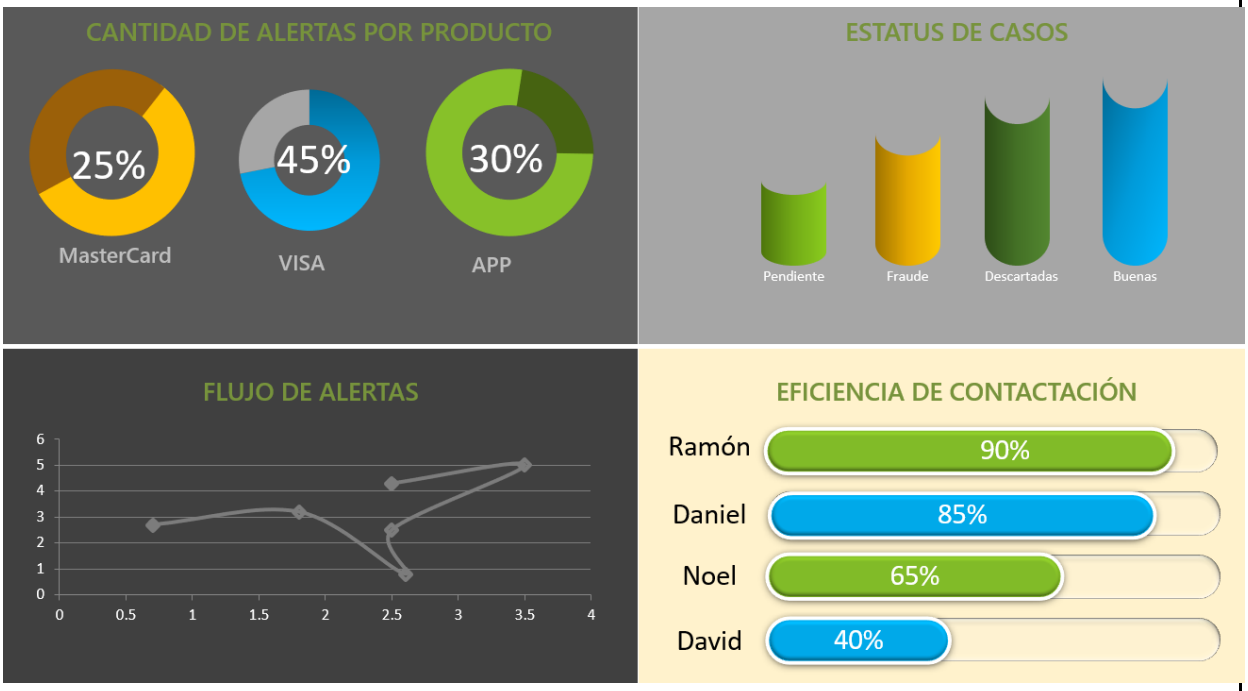
Fuente: creación propia

c) Gráficos

La información del tablero de mando deberá de ser proyectada simultáneamente en

gráficos adicionando la eficiencia de contactación por cada uno de los colaboradores, en donde ésta determinará al comparar la hora de la alerta contra la hora en que se confirmó, la cual si es en menos de 5 minutos es óptima, de 5 a 8 es deseable y de más de 8 es requiere mejora.

Figura 16. Gráficos.



Fuente: creación propia

6.4.2. Descripción y desarrollo de medidas a corto plazo.

6.4.2.1. Trabajo colaborativo

El área de operaciones en tarjetas está conformada por 28 colaboradores en los cuales existen 5 unidades o departamentos y es donde se localiza monitoreo y prevención de fraude conformada por el jefe y cinco analistas de prevención de fraude, en aras de eficiencia operativas es importante crear equipos multifuncionales para que de esta manera al momento de presentarse picos en algún horario o día especifico o bien por ataques masivos se puede incorporar un colaborador de los otros departamentos para que

de ésta amanera de garantice los tiempos de resolución de los casos así como garantizar el servicio a los clientes.

En consideración al incremento del 837% en las alertas derivadas de la transaccionalidad realizada por los clientes en el uso del APP, se analizaron las mismas para ello se consideró considerando el falso positivo actual y dimensionando rangos por score es por lo que se propone los siguientes cambios:

Figura 17. Análisis de mejora de alertas.

Regla	ACTUALIDAD			Propuesta	RESULTADOS ESPERADOS		
	Total, Alertado	Fraude	Falso Positivo		Total, Alertado	Fraude	Falso Positivo
Lista negra de usuarios	4,591	13	353	Depuración de 267 usuarios con alertas descartadas o buenas confirmadas por Monitoreo	1,054	13	81
Cambio de contraseña - Dispositivo diferente	4,557	5	911	Incremento de Score de 450 a 522	1,012	5	63
Cambio de contraseña - iPhone	1,705	0	1,705	Incremento de Score de 250 a 522	67	0	67
Retiros sin tarjeta	978	0	978	Modificación en la validación del Score a >=650	5	0	5
Login Lista de dispositivos	861	0	861	Al modificar las reglas de control de dispositivo se reduce un 75% el bloqueo de dispositivos	186	0	186
>1 usuario Mismo dispositivo	290 (75 clientes)	0	290	Eliminar de la lista el primer usuario	152 (35 clientes)	0	152
ACH Score alto	283	12	24	Incremento de Score de 700 a 790	175	12	15
Transferencia Monto alto	237	0	237	Agregar Score >=650	107	0	107
Lista de flujos administrativos	236	3	79	Ninguna modificación	236	3	79
Avance de efectivo	146	0	146	Eliminar regla	0	0	0
Total, alertas	**14,584**	**33**	**396**		**2,994**	**33**	**70**

Fuente: creación propia.

Esta actividad es aconsejable realizarla en una forma continua y replicarla a las alertas de los demás productos de manera de asegurar la carga laboral, importante el

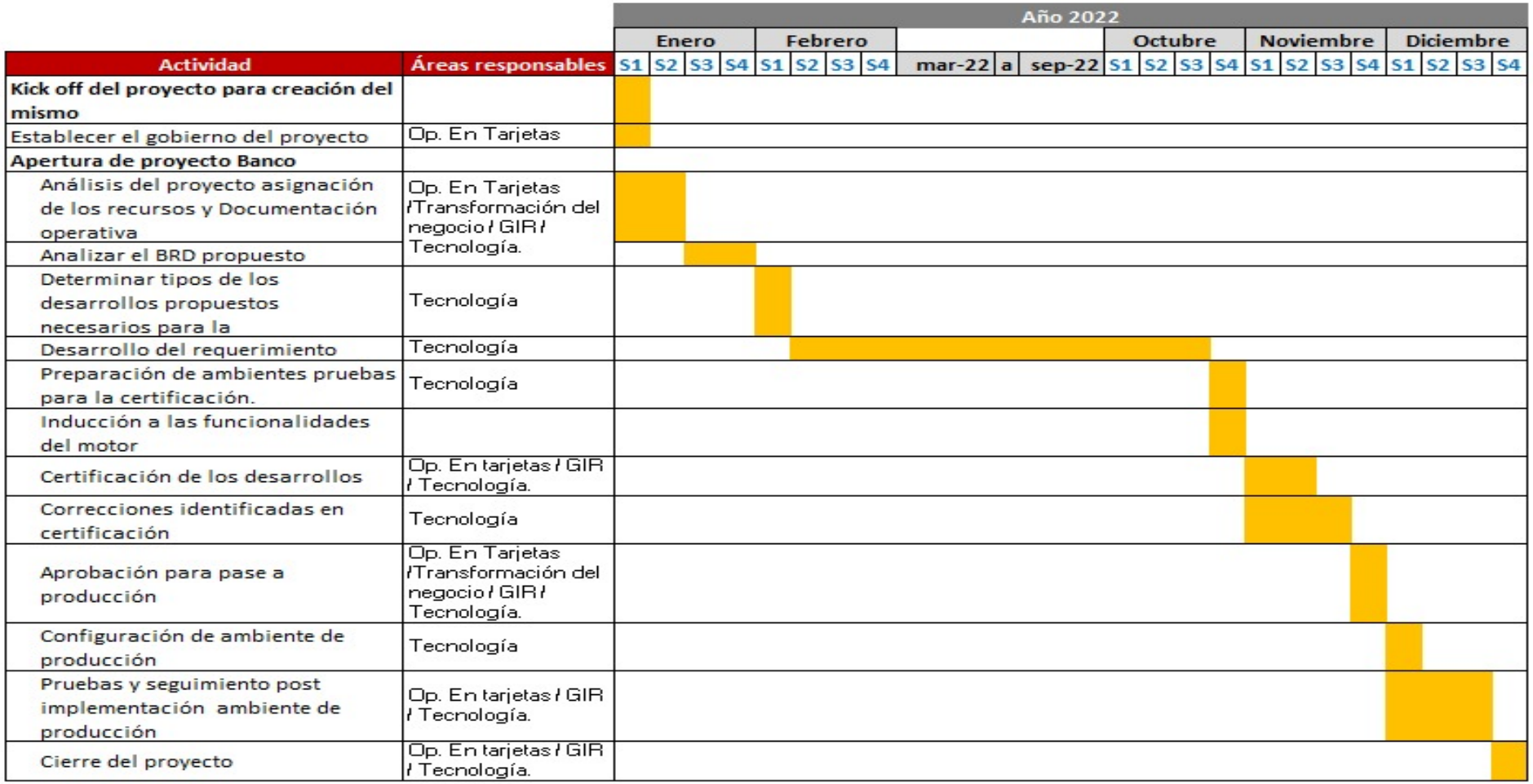
seguimiento de efectividad, traerá consigo la disminución del 40% del total de gestiones atendidas por usuarios digitales bloqueados que darán holgura en tiempo de 45 minutos por analista. De igual manera, en cuanto al seguimiento de las alertas pendientes, se estima una reducción de un 80%.

6.4.2.2. Capacitaciones

Debido a las necesidad identificada en el proceso de indagación es necesario profundizar en temas de análisis de fraudes específicamente en lo que la industria cibernéticos y forenses para ello se debe de someter al área de talento humano requerimiento para dicho curso así como una evaluación de la descripción de puestos de manera de que el grado académico que se requiera sea de licenciatura de administración de la tecnología o bien carreras afines, igual agregar alto nivel de maneo de ella mientas tecnológicas considerando el análisis de información de que siempre está expuesto el analista.

6.5. Cronograma de implementación y presupuesto

6.5.1. Cronograma de implementación



Actividad	Áreas responsables	Año 2022																					
		Enero				Febrero								Octubre				Noviembre				Diciembre			
		S1	S2	S3	S4	S1	S2	S3	S4	mar-22	a	sep-22		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Kick off del proyecto para creación del mismo																									
Establecer el gobierno del proyecto	Op. En Tarjetas																								
Apertura de proyecto Banco																									
Análisis del proyecto asignación de los recursos y Documentación operativa	Op. En Tarjetas /Transformación del negocio / GIR / Tecnología.																								
Analizar el BRD propuesto																									
Determinar tipos de los desarrollos propuestos necesarios para la	Tecnología																								
Desarrollo del requerimiento	Tecnología																								
Preparación de ambientes pruebas para la certificación.	Tecnología																								
Inducción a las funcionalidades del motor																									
Certificación de los desarrollos	Op. En tarjetas / GIR / Tecnología.																								
Correcciones identificadas en certificación	Tecnología																								
Aprobación para pase a producción	Op. En Tarjetas /Transformación del negocio / GIR / Tecnología.																								
Configuración de ambiente de producción	Tecnología																								
Pruebas y seguimiento post implementación ambiente de producción	Op. En tarjetas / GIR / Tecnología.																								
Cierre del proyecto	Op. En tarjetas / GIR / Tecnología.																								

6.5.2. Presupuesto

Detalle	Costo
Curso de especialización de fraudes 7 personas	L 84,950
Habilitación de colas MQ con SISCARD, para interrelación de transacciones en línea.	L 60,675
Horas de desarrollo de parte del equipo técnico, son 1,015 horas a un costo de L. 1,214	L 1,231,703
Talento Humano del Banco Involucrado en el Proyecto	L 250,000
Total, requerido	**L 1,627,328**

Este presupuesto oscila en un 29% en comparación a las pérdidas materializadas en el año 2020. La ejecución de ésta propuesta, minimizará el riesgo operativo así como optimizará los recursos de la institución como de igual forma, la eficiencia en la ejecución del proceso, garantizando el control sobre los alertamientos de fraude.

6.6. Concordancia de los segmentos de la tesis con la propuesta.

Capítulo 1			Capítulo II	Capítulo III			Capítulo V	Capítulo IV	
Título de la investigación	Objetivo General	Objetivos Específicos	Teorías de sustento	Variables	Población	Técnicas	Conclusiones	Nombre de la propuesta	Objetivos de la propuesta
Propuesta de herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras	Proponer los requerimientos necesarios para la selección de una herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras, mediante la indagación de la tecnología, controles y la experiencia de personas involucrados en el proceso y tema, para apoyar en la eficiencia de los controles de riesgos operativos y el servicio al cliente, así como el mantenimiento de una carga laboral óptima.	Conocer los factores que influyen en el proceso ejecutado por Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.	Teoría General de la Administración	Factores Motores de análisis Comportamiento transaccional	11 expertos en el tema de investigación	Entrevista	En la presente investigación se confirmaron y se detallaron los diferentes factores actuales que influyen en el proceso de monitoreo y prevención de fraude, mismos que son considerados por los analistas y personas involucradas en el proceso, de igual forma se identifican algunos que las herramientas actuales no tienen, dando oportunidades para ser incluidos, todo esto conlleva un panorama más amplio para la propuesta que deberá de afirmar la seguridad y agilidad en las actividades, convirtiéndose en los beneficios que apoyen a los	Motor Integrador de Fraude Davivienda.	Proporcionar un documento de requisitos comerciales (BRD por sus siglas en inglés) al área de operaciones en tarjetas de Davivienda para que le sirva de guía en la solicitud de desarrollo de un motor integrador de fraude.

Continuidad de tabla

							efectos identificados.		
		Determinar los requerimientos técnicos, regulatorios y políticas que debe de contener un sistema de información que Davivienda pueda utilizar para la prevención de fraudes en los canales digitales y comercios.	Teoría sobre la Seguridad Informática	Requerimientos técnicos, regulatorios y políticas. Reglas Reformas Aplicabilidad.	5 analistas del proceso de monitoreo y prevención de fraudes	Observación	Existen regulaciones emanadas por la CNBS y leyes que el estado de Honduras ha generado, en donde algunos artículos específicos repercutan en la ejecución del proceso de monitoreo y prevención de fraude, de igual forma a lo interno Davivienda tiene establecido una apolítica que genera las directrices necesarias en el establecimiento de las reglas de alertamientos transaccional, sin embargo se pudo constatar que algunas de las personas involucradas en el proceso no las conocen a profundidad, lo que podría presentar problemática al		Asegurar bajo esta herramienta el cumplimiento oportuno de las normas, leyes y regulaciones, específicamente los artículos vinculados al fraude, adhiriendo al motor integrador de fraude directrices y parámetros.

Continuidad de tabla

							momento de los análisis, para esta investigación fue de importancia establecer estos elementos para ser considerado en la propuesta.		
		Considerar el proceso de gestión de tecnología e innovación para la propuesta de una herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.	Teoría de Gestión de Tecnología e Innovación	Proceso de gestión de tecnología. Sistemas de seguridad. Controles Personas.			A través de la investigación se demostró que el proceso de monitoreo y prevención de fraude contiene ciertas debilidades o aspectos que podrían ser reforzados o mejorados entre algunas; la contactación de los clientes, evaluación oportuna de eficiencia de las alertas y múltiples herramientas para el análisis. Con esto podemos indicar que por medio de la tecnología emergente y la innovación se puede obtener aportes sustanciales que apoyaron esta propuesta.		Optimizar el proceso de monitoreo y prevención de fraude, utilizando el motor integrador, el cual permitirá la reducción de los tiempos de contactación del 20.5% en alertamientos de tarjetas de crédito y débito, un 23% para APP y en cuanto a generación de métricas un 100%, asegurando un porcentaje de contactación y gestión del 98% mínimo.

Continuidad de tabla

		Diseñar una propuesta de herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios.		Herramienta integradora. Experiencia de los expertos. Presupuesto. Tiempo.			Esta investigación obtuvo de los involucrados en el procesos de monitoreo y prevención de fraude, así como expertos nacionales e internacionales conocedores de fraudes y de sistemas medios de pagos, un detalle de componentes, elementos y directrices que se deben de considerar al diseñar un prototipo de una herramienta integradora de análisis de transacciones fraudulentas, los expertos indicaron cuan importantes es que toda organización invierta en desarrollos para este tipo de sistemas.		Plantear el diseño para una propuesta de herramienta integradora que pueda utilizar Davivienda para el monitoreo y prevención de fraudes en los canales digitales y comercios. Proponer medidas a corto plazo que apoyarán al proceso y generarán motivación al talento humano, a través de evaluación de las alertas de APP con una reducción del 81%, el trabajo colaborativo, capacitaciones y una evaluación de descripción de puestos. Rentabilizar los recursos y sistemas de información que ya cuenta el banco, de manera de utilizar en la generación de esta herramienta que apoyara en la mitigación de fraude.

REFERENCIAS BIBLIOGRÁFICAS

Banco Mundial. (8 de junio de 2020). Obtenido de https://www.bancomundial.org/es/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii

BID; OEA. (2020). *CIBERSEGURIDAD.* Banco de Interamericano de Desarollo. Recuperado el 29 de octubre de 2021, de https://publications.iadb.org/es/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Castro, J. (09 de julio de 2021). Obtenido de https://blog.corponet.com.mx/que-es-la-inteligencia-de-negocios

Chiabenato, I. (2008). *Gestión de Talento Humano* (Vol. tercera edición). México D.F: McGraw Hill. Recuperado el 24 de noviembre de 2021, de https://cucjonline.com/biblioteca/files/original/338def00df60b66a032da556f56c28c6.pdf

CNBS. (12 de noviembre de 2012). *Normas para el fortalecimiento de la transparencia, la cutura financiera y atención al usuario financiero en las instituciones supervisadas*. Tegucigalpa, Honduras.

CNBS. (2021). *Comisión Nacional de Bancos y Seguros*. Obtenido de https://publicaciones.cnbs.gob.hn/boletines/_layouts/15/xlviewer.aspx?id=%2Fboletines%2FRanking%20NIIF%2FRanking.xlsx&Source=https%3A%2F%2Fpublicaciones.cnbs.gob.hn%2Fboletines%2FPaginas%2FRanking-NIIF.aspx&action=edit

CNBS. (30 de 10 de 2021). *www.cnbs.gob.hn*. Obtenido de https://www.cnbs.gob.hn/sitios-relacionados-enlaces-de-interes/

Davivienda . (octubre de 2021). Honduras.

Díaz, G., & Espinoza, D. (2018). La innovación: baluarte fundamental para las organizaciones. *INNOVA Research Journal*, 214. Obtenido de file:///C:/Users/ferna/Downloads/Dialnet-Innovation-6792584.pdf

Díaz, J., & Romero, E. (2010). El uso del diagrama causa-efecto. *Revista Latinoamericana de Estudios Educativos (Mexico)*, 128.

FBI. (2020). *Internet Crime Report.* Técnico , IC3. Recuperado el 20 de 10 de 2021, de https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

FOSDEH. (2021). *Honduras, globalización y la aventura de las ZEDES.* Tegucigalpa. Recuperado el noviembre de 2021, de ttps://fosdeh.com/wp-content/uploads/2021/05/fosdeh-2021-aventura-ZEDES.pdf

Gaceta, L. (10 de mayo de 2019). Código Penal. Tegucigalpa, Honduras.

García, F. (2015). La Tegnología. *Revista de la Asociación Mexicana de Metodología de la Ciencia y de la Investigación, A.C.*, 14. Obtenido de http://www.ammci.org.mx/revista/pdf/Numero2/2art.pdf

Gómez, M. (2016). *Manual de Control Administrativo.* INEGI. Obtenido de https://silo.tips/download/manual-de-control-administrativo

Grupo Bolivar. (30 de 10 de 2021). *www.grupobolivar.com.* Obtenido de https://www.grupobolivar.com.co/wps/portal

ICE. (2021). *www.ice.gov*. Recuperado el 29 de 10 de 2021, de U.S. Immigration and customs Enforcement: https://www.ice.gov/es/investigaciones/delitos-ciberneticos#

INSL. (2018). *Riesgos por carga, física o mental, de trabajo.* Obtenido de http://www.navarra.es/NR/rdonlyres/74D4E0EE-0BD0-43E1-91BC-235B883C85B1/0/m2ud3.pdf

La Gaceta. (2 de agosto de 2017). Ley de tarjeta de crédito . Tegucigalpa, Honduras.

López, C. (2019). *DIFERENCIA ENTRE SEGURIDAD INFORMATICA Y CIBERSEGURIDAD.* Obtenido de http://polux.unipiloto.edu.co:8080/00004637.pdf

López, J. (20 de noviembre de 2021). *Economipedia*. Obtenido de https://economipedia.com/definiciones/proceso-administrativo.html

Lutkevich, B. (1 de 11 de 2021). *TechTarget.* Obtenido de https://www.computerweekly.com/es/definicion/Tokenizacion

Martínez, A. (2010). EL SÍNDROME DE BURNOUT. EVOLUCIÓN CONCEPTUAL Y ESTADO ACTUAL DE LA CUESTIÓN. *Vivat Academia*, 47. Obtenido de https://www.redalyc.org/pdf/5257/525752962004.pdf

Molina, A. d. (2019). *Conexionesan.* Obtenido de https://www.esan.edu.pe/apuntes-empresariales/2019/02/4-pasos-para-implementar-un-sistema-de-seguridad-de-información/

Orellana, G. (29 de 10 de 2021). Vicepresidente Comité de Fraude AHIBA. (R. Rivera, Entrevistador)

Ortíz, E., & Nagles García, N. (2013). *Gestión de Tecnología e Innovacíon.* Bogotá: Ediciones EAN. Obtenido de https://editorial.universidadean.edu.co/acceso-abierto/gestion-de-tecnología-e-innovación-ean.pdf

PayPal. (2021). *América Latina y el desafío de la seguridad digital - Combatiendo el fraude en un mundo digitalizado.* Recuperado el 29 de 10 de 2021, de https://www.paymentmedia.com/news-5316-amrica-latina-y-el-desafo-de-la-seguridad-digital---combatiendo-el-fraude-en-un-mundo-digitalizado.html

Ritzman, L., Malhotra, M., & Krajewski, L. (2008). Administración de Operaciones. Mexico: PEARSON EDUCACIÓN. Obtenido de file:///C:/Users/ferna/Desktop/Maestria/Dirección%20en%20Tecnología%20y%20las%20Operaciones/Administración_De_Operaciones_LEE_J_KRAJ.pdf

Rodriguez, E. j. (2021). *La Pobreza Codiciones estrectural Limitante para el desarollo económico y social del pasi.* UNAH. Recuperado el 30 de 10 de 2021, de https://presencia.unah.edu.hn/noticias/tasa-de-pobreza-en-honduras-paso-del-59-3-en-el-2019-a-70-en-el-2020-indica-boletin-economico-de-la-unah/

Sampieri, R., Fernández, C., & Baptista, M. (2014). Metodología de la Investigación. Mexico: Mc Graw Hill Education.

TODO1. (2021). *TODO1 servicios*. Obtenido de https://www.todo1services.com/

Torres, Z. (2014). *Teoría General de la Administración* (segunda edicion ed.). Mexico: Grupo Editorial Patria. Obtenido de https://books.google.hn/books?id=LtLhBAAAQBAJ&pg=PR3&hl=es&source=gbs_selected_pages&cad=3#v=onepage&q&f=false

TransUnion. (21 de 07 de 2020). *newsroom.transunion.com.* Recuperado el 2021, de https://newsroom.transunion.com/transunion-enhances-document-verification-solution-as-new-research-finds-identity-fraud-at-center-of-many-digital-covid-19-scams/

GLOSARIO

Alerta: resultado de un análisis de información que dan los avisos para que pueda evaluarse un acto específico considerado de riesgo.

Autorización: proceso que da por aprobado un acto en ejecución por una persona.

Chip: dispositivo de seguridad instalado en una tarjeta de crédito y débito u otros aparatos que generan coordenadas de autenticidad

Consumo: acción que se ejerce para obtener un producto o servicio.

Contactación: acto de comunicación verbal o escrita entre dos personas en donde una es el emisor y busca bajo cualquier medio al receptor de manera de indagar sobre una acción realiza por este.

Core bancario: sistema de información adherido por una organización para administrar los diferentes procesos necesarios en la vida de la misma, el cual está conformado por módulos que interactúan entre sí.

Dashboard: cuadro de mando que presenta de forma de gráfica, información relevante para un análisis.

Datas: archivos electrónicos que almacenan un sin números de campos que son necesarios en un sistema de información.

Declinada: es el actor de no aceptar un transacción o bien cualquier operación realizada por el cliente.

Defraudadores: personas que realizan actos ilegales con el fin de obtener un beneficio, perjudicando para ello a otras personas.

Falso positivo: es el punto de confianza del conjunto de alertamientos que se dan en un proceso de confirmación transaccional.

Infraestructura: las tecnologías que interfieren y gestiona los diferentes proceso informativos y de comunicación, interactuando entre sí de manera de complementos.

Inteligencia social: habilidad que utilizan los defraudadores para obtener información personal de sus víctimas.

Licenciamiento: es el permiso otorgado a un tercero para actuar en nombre de alguien o una empresa de manera afiliativa.

Logaritmos: conjunto de ecuaciones cuya solución dará como resultado un dato que es la solución única esperada en la ejecución de un proceso que está dentro de un sistema de información.

Perfil: es un detalle de la información básica o determinada de una persona en donde denota su gusto y preferencia, colocándolo en una clasificación o nivel.

Plataforma digital: son espacios en internet que permiten la ejecución de diversas aplicaciones, sistemas o programas en un mismo lugar y que las mismas satisfacen las necesidades de los usuarios o clientes.

Sitios Web: Conjunto de archivos electrónicos y páginas web que interactúan entre sí para mostrar información sobre un tema en particular.

Tercerización: acción que lleva a cabo una empresa al contratar otra empresa para que ejecute o administre uno o más procesos de su organización de manera de hacerlo más rentables y eficientes.

Transaccionalidad: es un conjunto de transacciones realizadas como una componente cuyo resultado final es una acción que manipula o genera una base de datos.

Transformación digital: es el cambio que conlleva la integración de la tecnología digital a un proceso o acciones realizadas por una empresa con la finalidad de adherir valor a sus clientes.

Usuario: persona que da uso a un producto o servicio financieros.

ANEXOS.

Anexo 1. Posición del sistema de bancos comerciales. Al mes de agosto 2021.

POSICIÓN DEL SISTEMA DE BANCOS COMERCIALES
(Cifras en Miles de Lempiras)
Al 30 de Septiembre del 2021

INSTITUCIONES	Activos Totales		Cartera Crediticia		Depósitos		Capital y Reservas		Utilidades	
	Saldo	Posición	Saldo	Posición	Saldo	Posición	Saldo	Posición	saldo	Posición
BANCO FINANCIERA COMERCIAL HONDURENA, S.A.	143,976,460.5	1	80,879,258.5	2	76,216,174.2	2	8,688,675.2	2	916,119.7	1
BANCO ATLANTIDA, S.A.	137,233,079.3	2	86,071,587.4	1	99,668,419.8	1	10,673,433.1	1	801,136.6	2
BANCO DE AMERICA CENTRAL HONDURAS, S.A.	114,048,362.5	3	57,787,667.5	3	75,375,308.0	3	8,005,248.3	4	673,655.2	3
BANCO DE OCCIDENTE, S.A.	110,674,255.6	4	42,926,715.4	5	72,569,003.1	4	8,369,231.9	3	531,042.3	5
BANCO DEL PAIS, S.A.	70,594,533.5	5	44,703,698.1	4	45,000,840.5	5	5,465,316.0	5	627,956.4	4
BANCO DAVIVIENDA HONDURAS, SOCIEDAD ANONIMA	43,980,757.3	6	30,380,180.5	6	26,278,394.9	6	3,340,936.1	6	245,942.0	6
BANCO LAFISE, HONDURAS	22,098,416.0	7	11,172,467.8	8	14,909,385.8	7	941,342.7	11	168,781.9	7
BANCO DE DESARROLLO RURAL S.A.	21,648,564.2	8	14,318,218.4	7	14,096,572.4	8	1,955,413.5	7	-232,861.0	15
BANCO PROMERICA, S.A.	16,748,688.5	9	9,685,827.9	9	10,497,893.7	9	1,182,142.4	9	28,911.2	14
BANCO FINANCIERA CENTROAMERICANA, S.A.	15,202,560.0	10	8,822,772.4	10	6,054,789.0	11	1,075,442.2	10	61,846.3	10
BANCO DE LOS TRABAJADORES, S.A.	9,280,509.2	11	6,372,823.5	11	7,399,339.2	10	855,505.4	13	49,120.9	11
BANCO DE HONDURAS, S.A.	7,388,726.7	12	1,455,716.6	15	3,981,740.5	12	925,325.4	12	152,614.9	8
BANCO AZTECA DE HONDURAS, S.A.	5,287,959.7	13	1,924,102.9	13	2,085,530.0	15	1,855,415.0	8	63,283.3	9
BANCO HONDURENO DEL CAFE, S.A.	5,053,298.2	14	1,525,386.5	14	3,389,344.6	13	665,156.0	15	30,048.7	13
BANCO POPULAR, S.A.	4,017,150.6	15	3,292,319.2	12	2,285,166.5	14	681,948.4	14	46,277.8	12
TOTALES	**727,233,321.9**		**401,318,742.6**		**459,807,902.4**		**54,680,531.5**		**4,163,876.4**	

Nota: Cifras preliminares publicadas bajo el marco contable basado en Normas Internacionales de Información Financiera (NIIF) combinadas con las Normas Prudenciales, mismas que tienen como fuente la información recibida del Sistema Supervisado y están sujetas a revisión posterior por parte de la CNBS.

Fuente: (CNBS, 2021)

Anexo 2. Instrumento de investigación: Encuesta.

GUIA DE ENTREVISTA

Buenos días / tardes / Noches

Somos estudiantes de la carrera de **Dirección Empresarial** en el grado de Maestría, en esta ocasión estamos realizando esta entrevista que nos ayudará en el proyecto de investigación sobre una herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras, nuestra intención es tener de usted esas experiencias y conocimientos que aporten a este estudio.

Antes de empezar necesito confirmar que no hay inconveniente en que grabemos la entrevista. Es solo a fines de facilitar la documentación, esta información no se va a compartir ni publicar en ningún sitio.

Datos Generales

Nombres y Apellidos: _____

Cuál es su puesto: _____

Años de laborar en Davivienda: _____

Años de experiencias: _____

Profesión: _____

Preguntas

1. ¿Cuáles son las herramientas que se utilizan en el proceso de análisis y prevención de fraudes?
2. ¿Conoce usted una herramienta ya existente en la industria o mercado que integre lo expuesto anteriormente? ¿Si los hay podría compartir el nombre de empresas que prestan este servicio?
3. ¿Cuáles son los datos mínimos requeridos para el análisis de una alerta?
4. ¿Cuáles son las políticas, regulaciones y normas que considera en un proceso de monitoreo y prevención de fraudes?
5. ¿Cuáles son las métricas que se generan para la evaluación del proceso de monitoreo y prevención de fraudes?
6. ¿Qué factores o elementos que deben de conjugar en una herramienta de monitoreo y prevención de fraudes?

7. ¿De acuerdo con su experiencia, qué prácticas y técnicas considera que debe de tener una herramienta de prevención de fraudes?
8. ¿Qué problemas considera usted se tiene en el proceso de monitoreo y prevención de fraudes?
9. ¿Qué propuestas y recomendaciones podría usted dar para una herramienta integradora de análisis y monitoreo de fraude?
10. ¿Considera usted importante tener una herramienta integradora donde se concentren los diferentes factores del proceso de monitoreo y prevención de fraude, así como tecnología involucradas en inteligencia de negocio?

Muchas gracias por compartir su experiencia, sin duda nos aportara elementos necesarios para mejorar

Anexo 3. Ficha de observación

FICHA DE OBSERVACIÓN

PROPUESTA DE HERRAMIENTA INTEGRADORA DE ANALISIS Y PREVENCIÓN DE FRAUDE PARA BANCO DAVIVIENDA HONDURAS.

Proceso Observado: Proceso de Monitoreo y prevención de fraude

Nombre Del Colaborador: _____

Nombre del Observador: _____

Horario realizado: _____

Fecha: _____

		Periodicidad			Requiere Supervisión			Tiene Control			
No.	Nombre de actividad	Diario	Semanal	Mensual	Otros	Si	No	Si	No	Tiempo Promedio	Observaciones

Comentarios Generales:

_____ _____ _____

Firma del colaborador Firma de jefe Firma del observador

Anexo 4. Carta de Autorización de la Empresa

CARTA DE AUTORIZACIÓN DE LA EMPRESA O INSTITUCIÓN

Tegucigalpa, Francisco Morazán, 3/12 /2021
(Cuidad), (Departamento) (Día, mes y año)

Rafael Cruz Castro
(Nombre y apellidos del Director o Gerente)

Subdirector de Operaciones
(Puesto Laboral)

Banco Davivienda Honduras S.A.
(Empresa o Institución)

Oficina principal, intersección Blvd. Suyapa y Blvd. Juan Pablo II.
(Dirección principal de la empresa o institución)

Estimado Señor(a): Cruz

Reciba un cordial y atento saludo. Por medio de la presente deseamos solicitar su apoyo, dado que somos alumnos de UNITEC y nos encontramos desarrollando el Trabajo Final de Graduación previo a obtener nuestro título de maestría en Dirección Empresarial.

Hemos seleccionado como tema "Propuesta de herramienta integradora de análisis y prevención de fraude para Banco Davivienda Honduras", por lo que estaríamos muy agradecidos de contar con el apoyo de la empresa que usted representa para poder desarrollar nuestra investigación. En particular, dicha solicitud se circunscribe a peticionar que se nos autorice a realizar: entrevistas y observaciones.

(encuestas, sondeos, etc).

A la espera de su aprobación, me suscribo de Usted.

Atentamente,

María Fernanda Rodriguez Rivera
No. de cuenta: 12013021

Ramón Alberto Rivera Villatoro
No. de cuenta: 12013302

Por este medio, Banco Davivienda Honduras S.A.
(Empresa / institución),
Autoriza la realización dentro de sus instalaciones el proyecto de investigación de Postgrado antes mencionado.

Rafael Cruz Castro
(Nombre y sello del Director / Gerente)

Vo.Bo