

Universidad de Lima  
Facultad de Ingeniería y Arquitectura  
Carrera de Ingeniería de Sistemas



# **PROTOTIPO DE DETECCIÓN DE FRAUDES CON TARJETAS DE CRÉDITO BASADO EN INTELIGENCIA ARTIFICIAL APLICADO A UN BANCO PERUANO**

Trabajo de suficiencia profesional para optar el Título Profesional de Ingeniero de Sistemas

**Cristian Andre Rayo Mondragon**

**Código 20112238**

**Asesor**

**Percy Diez Quiñones Panduro**

Lima – Perú

noviembre de 2020



**PROTOTYPE OF FRAUD DETECTION WITH  
CREDIT CARDS BASED ON ARTIFICIAL  
INTELLIGENCE APPLIED TO A PERUVIAN  
BANK**

# TABLA DE CONTENIDO

<b>RESUMEN.....</b>	<b>XII</b>
<b>ABSTRACT.....</b>	<b>XIII</b>
<b>CAPÍTULO I: INTRODUCCIÓN .....</b>	<b>1</b>
<b>CAPÍTULO II: FUNDAMENTOS TEÓRICOS .....</b>	<b>3</b>
2.1 Modalidades y tipos de fraudes .....	4
2.1.1 Phishing.....	4
2.1.2. Fraude por teléfono.....	5
2.1.3. “Regleta” .....	5
2.1.4. “Cambiazo” .....	5
2.2 Cybersecurity .....	5
2.3 Banca, canales y transacciones con tarjeta de crédito.....	6
2.4 Estadísticas relacionadas a bancos y operaciones con tarjeta de Crédito ....	10
2.5 Minería de Datos.....	16
2.6 Inteligencia Artificial .....	17
2.7 Machine Learning .....	17
2.8 Clasificación de sistemas de Aprendizaje Automático.....	17
2.9 Algoritmos de Machine Learning .....	17
2.9.1. Random Forest.....	18
2.9.2 Regresión Logística.....	20
2.9.3. Naive Bayes .....	21
2.9.4. Support Vector Machine.....	21

2.9.5.	K - Means Clustering.....	22
2.10	Matriz de confusión .....	22
2.11	Design Thinking .....	24
2.12	Componentes de arquitectura de solución .....	26
2.13	Metodología Ágiles .....	29
<b>CAPÍTULO III: FUNDAMENTACIÓN DEL PROYECTO.....</b>		<b>31</b>
3.1	Fundamentación de la deseabilidad del proyecto .....	31
3.2	Fundamentación de la factibilidad del proyecto .....	33
3.3	Fundamentos de la Viabilidad .....	36
3.3.1	Pérdidas económicas del banco con relación al fraude.....	36
3.3.2	Flujo de Caja .....	38
<b>CAPÍTULO IV: DEFINICIÓN DEL PROYECTO.....</b>		<b>42</b>
4.1	Definición del proyecto .....	42
4.1.1	Aliviadores de frustraciones y creadores de alegría.....	42
4.2	Objetivos del proyecto .....	44
4.3	Objetivo general.....	44
4.3.1	Objetivos específicos .....	44
4.4	Beneficios esperados .....	44
4.4.1	Costos totales del proyecto .....	44
4.5	Segmento de Mercado .....	45
4.6	Roles y responsabilidades del equipo del proyecto .....	46
4.7	Cronograma y riesgos iniciales del proyecto .....	48
4.8	Medidas de control (indicadores) .....	55
4.9	Recursos y presupuesto.....	55
<b>CAPÍTULO V: DESARROLLO DEL PROYECTO.....</b>		<b>58</b>
5.1	Empatizar .....	58

5.1.1	Entrevistas .....	58
5.1.2	Mapa de Empatía .....	60
5.2	Definir .....	61
5.3	Idear .....	62
5.3.1	Brainstorming.....	62
5.4	Prototipar .....	63
5.4.1	Prototipado de la solución.....	64
5.5	Testear.....	74
<b>CONCLUSIONES.....</b>		<b>75</b>
<b>RECOMENDACIONES.....</b>		<b>76</b>
<b>GLOSARIO .....</b>		<b>77</b>
<b>REFERENCIAS.....</b>		<b>79</b>
<b>BIBLIOGRAFÍA.....</b>		<b>82</b>
<b>ANEXOS.....</b>		<b>82</b>

## ÍNDICE DE TABLAS

Tabla 2.1 <i>Flujo de Proceso de Autorizaciones</i> .....	9
Tabla 2.2 <i>Evolutivo de transacciones por comercio electrónico (enero 2019 - agosto 2019)</i> .....	11
Tabla 2.3 <i>Evolutivo de transacciones por comercio electrónico (setiembre 2019 - junio 2020)</i> .....	11
Tabla 2.4 <i>Importe de transacciones por comercio electrónico (enero 2019 - agosto 2019)</i> .....	12
Tabla 2.5 <i>Importe de transacciones por comercio electrónico (setiembre 2019 - enero 2020)</i> .....	13
Tabla 2.6 <i>Importe de transacciones por comercio electrónico (febrero 2020 - junio 2020)</i> .....	13
Tabla 3.1 <i>Monto monetario recuperado y perdido</i> .....	37
Tabla 3.2 <i>Pérdidas monetaria por comercio electrónico</i> .....	37
Tabla 3.3 <i>Retorno de inversión (agosto 2020 - diciembre 2020)</i> .....	39
Tabla 3.4 <i>Flujo de caja (enero 2021 - mayo 2021)</i> .....	39
Tabla 3.5 <i>Flujo de caja (junio 2021 - octubre 2021)</i> .....	40
Tabla 3.6 <i>Flujo de caja (noviembre 2021 - marzo 2022)</i> .....	40
Tabla 3.7 <i>Flujo de caja (abril 2022 - agosto 2022)</i> .....	40
Tabla 3.8 <i>Flujo de caja (setiembre 2022 - diciembre 2022)</i> .....	41
Tabla 4.1 <i>Costo de la solución</i> .....	45
Tabla 4.2 <i>Cronograma de actividades</i> .....	50
Tabla 4.3 <i>Historia de Usuario - Ingreso al sistema como usuario administrador</i> .....	51
Tabla 4.4 <i>Historia de Usuario - Gestión de usuarios al sistema</i> .....	51

Tabla 4.5 <i>Historia de Usuario - Gestión de cambio de contraseña</i> .....	51
Tabla 4.6 <i>Historia de Usuario - Exportar data en archivo excel</i> .....	52
Tabla 4.7 <i>Historia de Usuario - Notificar alertas que llegan al sistema</i> .....	52
Tabla 4.8 <i>Historia de Usuario - Marcaje manual de fraude en visor</i> .....	52
Tabla 4.9 <i>Historia de Usuario - Generación de Informe de indicadores de fraude</i> .....	53
Tabla 4.10 <i>Historia de Usuario - Ingresar comentario como referencia a las transacciones gestionadas</i> .....	53
Tabla 4.11 <i>Product Backlog</i> .....	54
Tabla 5.1 Preguntas de Entrevista.....	59
Tabla 5.2 <i>Definición de variables</i> .....	67
Tabla 5.3 <i>Resultados Matriz de Confusión</i> .....	72



## ÍNDICE DE FIGURAS

Figura 2.1	<i>Componentes del Triángulo del Fraude</i> .....	4
Figura 2.2	<i>Canales del banco</i> .....	7
Figura 2.3	<i>Ciclo de una transacción</i> .....	9
Figura 2.4	<i>Cantidad de transacciones por comercio electrónico</i> .....	12
Figura 2.5	<i>Importe de Transacciones por comercio electrónico</i> .....	13
Figura 2.6	<i>Transacciones fraudulentas - ECI 7</i> .....	14
Figura 2.7	<i>Cantidad de Reclamos (2018-2019)</i> .....	15
Figura 2.8	<i>Pérdidas anuales totales</i> .....	16
Figura 2.9	<i>Técnica y/o modelo Minería de Datos</i> .....	18
Figura 2.10	<i>Diagrama Random Forest</i> .....	19
Figura 2.11	<i>Función Sigmoide</i> .....	20
Figura 2.12	<i>Support Vector Machine</i> .....	22
Figura 2.13	<i>Matriz de Confusión</i> .....	23
Figura 2.14	<i>Factores Design Thinking</i> .....	26
Figura 2.15	<i>Componentes Spark Streaming</i> .....	27
Figura 2.16	<i>Arquitectura de Solución</i> .....	28
Figura 3.1	<i>Lienzo Model Canvas</i> .....	34
Figura 4.1	<i>Lienzo propuesta de valor</i> .....	43
Figura 5.1	<i>Mapa de Empatía</i> .....	61
Figura 5.2	<i>Brainstorming</i> .....	63
Figura 5.3	<i>Pantalla de Login</i> .....	65

Figura 5.4 <i>Visor de transacciones fraudulentas</i> .....	66
Figura 5.5 <i>Visor de Reportes Estadísticos</i> .....	66
Figura 5.6 <i>Visualización de datos</i> .....	69
Figura 5.7 <i>Transformación de Datos</i> .....	70
Figura 5.8 <i>Normalización de los datos</i> .....	71
Figura 5.9 <i>Modelo Pipeline</i> .....	72
Figura 5.10 <i>Interfaz de MVP</i> .....	74

## ÍNDICE DE ANEXOS

Anexo 1 : Flujo de procesos del prototipo desarrollado .....	82
Anexo 2 : Código fuente - Entrenamiento Algoritmo Random Forest .....	84
Anexo 3 :Código fuente - entrenamiento algoritmo Random Forest (separación de data de prueba y validación).....	84
Anexo 4: Código fuente – Matriz de Confusión .....	85
Anexo 5: Código fuente – Matriz de Confusión .....	85
Anexo 6: Código fuente – Algoritmo Random Forest.....	86
Anexo 7: Código fuente – Visor de Transacciones Fraudulentas.....	86
Anexo 8: Código fuente – Visor de Transacciones Fraudulentas.....	87

## RESUMEN

El presente trabajo está centrado en el área de prevención y tratamiento del fraude de un banco peruano. Esta organización brinda servicios y soluciones financieras a sus clientes a través de sus diferentes canales de atención, siendo el canal de ventas por comercio electrónico el más vulnerable y el más crítico, debido a que el número de fraudes identificados por este canal se ha incrementado significativamente en el contexto pandemia - COVID 19. Existen varias formas de cometer fraudes, una de las más comunes es a través de la captura de la información de la tarjeta del cliente por “phishing”, robo o hurto desde el teléfono del cliente, el cual suele encontrar información importante como el registro de sus tarjetas en aplicativos móviles, etc.

Actualmente, el banco cuenta con la herramienta Visa Risk Manager, la cual permite a los analistas de fraudes pueden crear reglas de fraude para rechazar o alertar transacciones sospechosas en base a criterios relacionados a los montos, tipos de comercio, entre otros.

El comportamiento de los clientes y sus patrones de consumo son variables muy volátiles y un analista de fraudes no es capaz de poder responder rápidamente a estos cambios. Por ello, es necesario que dicho analista de fraude cuente con una herramienta o plataforma basada en Machine Learning, el cual detecte el fraude a través del canal de comercio electrónico en tiempo real, y no depender de reglas estáticas preconfiguradas.

El modelo de detección de fraudes se basó en la aplicación del algoritmo Random Forest, para esto, se optó por separar el set de datos, donde el 80% corresponde a data para el entrenamiento del modelo y el 20% restante para validación y pruebas. Los resultados experimentales sobre el conjunto de datos de pruebas muestran que el modelo tiene una precisión del 48.10% con un falso positivo de 4.35, que irá mejorando a partir del aumento del volumen transaccional y la ejecución progresiva del modelo a partir de la data entrante.

### **Palabras clave:**

Visa Risk Manager, Machine Learning, Random Forest, Aprendizaje Supervisado, Aprendizaje no supervisado, Design Thinking

## ABSTRACT

This paper focuses on the fraud prevention and treatment area of a peruvian bank. This financial institution provides financial services and solutions to its customers through its different customer service channels, being the e-commerce sales channel being the most vulnerable and the most critical, because the number of frauds identified through this channel has increased significantly in the context of the pandemic - COVID 19. There are several ways to committing fraud, one of the most common is through the capture of the customer's card information by "phishing", robbery or theft of the customer's phone, which usually finds important information such as the registration of their cards in mobile applications, etc.

Currently, the bank has a Visa Risk Manager tool, which allows fraud analysts to create fraud rules to reject or alert suspicious transactions based on criteria related to amounts, types of merchant name, among others.

Customer behavior and consumption patterns are highly volatile variables and a fraud analyst is not able to respond quickly to these changes. Therefore, it is necessary that the fraud analyst has a tool or platform based on Machine Learning, which detects fraud through the e-commerce channel in real time and does not rely on static preconfigured rules.

The fraud detection model was based on the application of the Random Forest algorithm, for this, it was decided to separate the data set, where 80% corresponds to data for model training and the remaining 20% for validation and testing. The experimental results on the test data set show that the model has an accuracy of 48.10% with a false positive of 4.35, which will improve as transaction volume increases and progressive execution of the model from the incoming data.

### **Keywords:**

Visa Risk Manager, Machine Learning, Random Forest, Supervised Learning, Unsupervised Learning, Design Thinking



# CAPÍTULO I: INTRODUCCIÓN

Actualmente, estamos viviendo con tendencias como revolución 4.0 o Transformación Digital, lo cual implica que todas las organizaciones hacen uso de las nuevas tecnologías para apoyarse y poder gestionar todos sus procesos de negocios orientados a la satisfacción del cliente.

Según las estadísticas recopiladas por el Centro de Denuncias de Delitos por Internet (IC3) del FBI, durante el 2018, el robo, fraude y la explotación por internet, fueron responsables de 2,700 millones de dólares en pérdidas financieras.

Las transacciones financieras por canales digitales crecieron, solamente en América Latina, casi un 50% desde que se decretó el aislamiento social obligatorio a raíz de la pandemia por COVID -19, lo que significa que el índice de riesgo sigue esa misma tendencia de crecimiento. Asimismo, han surgido nuevas formas de fraude y robo de información, tales como páginas falsas relacionadas a datos de carácter informativo acerca de cantidad de personas contagiadas y personas que fallecieron a causa del COVID -19, sitios web que, al ser abiertos, instalan automáticamente virus y malware en dispositivos móviles o computadoras. Estos programas se encargan de robar la información sensible del usuario tales como datos personales, información bancaria, y otros, que quedan expuestas en manos de delincuentes informáticos para cometer actos fraudulentos.

El 39% de los peruanos desconfía que los productos comprados vayan a ser entregados de manera correcta en su domicilio (Bambarén, sección de Economía, 2019, párr. 3).

Existen razones de la desconfianza del peruano al hacer compras por internet, tales como, por ejemplo, el miedo a que su información se encuentre expuesta al brindar sus datos personales, por lo que prefiere hacer la compra en una tienda física.

El escenario económico actual en el Perú, durante el primer trimestre del año 2020, tiene proyecciones desalentadoras, a causa de la pandemia, que ha provocado el aislamiento social, cuarentena y consiguio la paralización de diversas actividades de la industria. La situación ha llevado a que las personas permanezcan en sus casas y estén forzadas a realizar operaciones y compras, a través de canales digitales.

Ante el incremento de dichas operaciones, estas se han convertido en un blanco atractivo y rentable para los defraudadores, quienes cometen fraudes mediante el robo de las credenciales de los usuarios genuinos (datos como número de tarjeta de Crédito, CVV y fecha de caducidad de la tarjeta) para realizar compras en los diversos comercios online que existen para beneficio propio y /o de terceros, perjudicando económicamente al usuario, ocasionando pérdidas económicas así como el desprestigio de la imagen de la institución financiera.

Por ello, la prevención y la detección del fraude en cualquiera de sus formas se ha convertido en un reto para todas las organizaciones independientemente de su tamaño, ya que la materialización de un fraude involucra altos costos para las compañías y sobre todo la pérdida del recurso intangible más valorado por el cliente: imagen y reputación.

El fraude en tarjetas de crédito representa una pequeña parte dentro del mundo del fraude a nivel general, y constituye un problema que tiene una curva ascendente en el tiempo, debido al incremento de ventas online, por lo que constituye un reto constante detectar oportunamente transacciones fraudulentas.

El motivo de la elaboración del presente proyecto de innovación tecnológica tiene como finalidad satisfacer las necesidades del analista y/o especialista de fraudes, mediante la implementación de una herramienta que permita detectar aquellas transacciones fraudulentas mediante el uso de la Inteligencia Artificial - Machine Learning, que, a través de la implementación y adaptación de algoritmos de aprendizaje automático Random Forest, pueda detectar e identificar transacciones fraudulentas.



## CAPÍTULO II: FUNDAMENTOS TEÓRICOS

Antes de abordar los fundamentos teóricos que respaldan nuestro proyecto, es importante comenzar definiendo el término “fraude”.

Según la *Association of Certified Fraud Examiners (ACFE)*, el fraude incluye cualquier acto intencional o deliberado de privar a otros, de bienes o dinero por astucia, engaño u otros actos injustos (Sadgal et al., 2019, p. 46).

El triángulo del fraude es un modelo desarrollado por el doctor Donald Cressey en 1991, bajo la casuística del por qué las buenas personas cometen fraudes.

Componente del “Triángulo del Fraude”:

- **Oportunidades Recibidas**

Componente relacionado a la oportunidad presentada cuando alguien tiene los accesos y conocimientos necesarios para cometer un fraude.

- **Motivo**

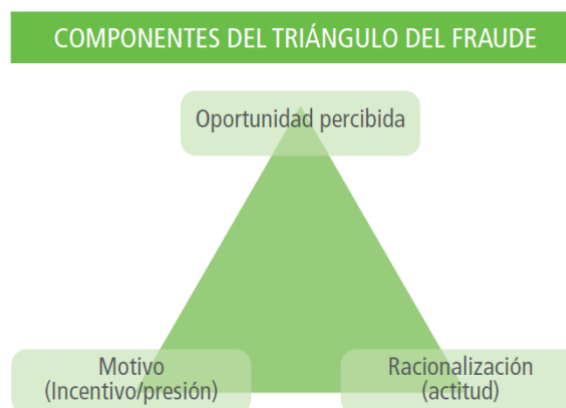
Componente relacionado a que los empleados de empresas tienen un estímulo o presión para cometer fraudes. Esto se puede dar, por ejemplo, cuando el colaborador quiere alcanzar las metas de desempeño (como volúmenes de ventas) o mantener su puesto demostrando resultados no reales o ficticios, entre otras posibilidades.

- **Racionalización**

Componente relacionado a que la persona que comete fraude se convenga así misma, de manera consciente o inconsciente, que existen razones válidas para justificar su comportamiento.

## Figura 2.1

### Componentes del Triángulo del Fraude



*Nota.* La figura representa los componentes del triángulo del fraude. Adaptado de Manual de Gestión del Riesgo del Fraude: Prevención, Detección e Investigación” por Instituto de Auditores Internos de España, 2015, p.17

## 2.1 Modalidades y tipos de fraudes

Las casuísticas por las cuales se puede llevar a cabo un fraude son diversas y dinámicas en el tiempo, ya que los defraudadores buscan nuevos mecanismos para poder robar la información de los tarjetahabientes para cometer fraudes. A continuación, se mencionan las modalidades más representativas.

### 2.1.1 Phishing

Es una modalidad de fraude utilizada por los defraudadores, que consiste en el envío de gran cantidad de correos electrónicos no deseados, a través de versiones falsas de sitios web, con la finalidad de convencer a las personas de que hagan clic en un enlace que los enviará al sitio web falso (Hussain et al., 2010, p. 234).

El creciente número de incidentes de phishing ha contribuido a aumentar las pérdidas por fraude bancario, ya que los clientes de los bancos son cada vez más propensos a este tipo de ataques. El software espía es un tipo de virus informático que se puede instalar en la computadora sin que el usuario se dé cuenta, dicho programa es capaz de actuar como un registrador de pulsaciones de teclas, capturando así todas las pulsaciones hechas en el

teclado de una computadora. Los correos electrónicos que son enviados están básicamente relacionados con la banca por internet e intentan engañar a las personas para que visiten o hagan clic en el enlace, que redirecciona a una página fraudulenta para el robo de sus datos personales. (Hussain et al., 2010, p. 234).

### **2.1.2 Fraude por teléfono**

Modalidad usada por los estafadores, para conseguir información sensible a través de llamadas telefónicas, haciéndose pasar por colaboradores de bancos u otras entidades financieras. Por otro lado, bajo este mismo canal, los defraudadores, llaman al usuario informándoles que han sido acreedores de un beneficio económico, para obtener dicho beneficio les exigen brindarles los datos de su tarjeta, cuenta, código CVV, entre otra información sensible.

### **2.1.3 “Regleta”**

Es una modalidad de fraude que consiste en manipular los cajeros automáticos y colocar objetos similares a una regla, en la zona, donde se dispensa el dinero, a fin de que se impida la salida de este para que, finalmente, el defraudador recoja el dinero retenido.

### **2.1.4 “Cambiozo”**

Esta modalidad de fraude consiste en que el defraudador busca distraer la atención del usuario y logra hacer el cambio de su tarjeta de crédito y /o débito por una de similares características y por lo general también obtienen la clave de la tarjeta.

## **2.2 Cybersecurity**

Con respecto a la ciberseguridad:

La ciberseguridad se define como la práctica de proteger a los aparatos de cómputo como, por ejemplo, las computadoras, servidores, dispositivos móviles, entre otros, a través de técnicas que permitan resguardar la

privacidad, integridad y la disponibilidad de los ordenadores y los datos frente a posibles amenazas ante la existencia de vulnerabilidades de los sistemas, identificados por los hackers para cometer un ataque. (Crashcourse, 2017).

El campo de la ciberseguridad ha evolucionado rápidamente, ya que existe la necesidad de estar a un paso por delante de los hackers, quienes diseñan nuevas estrategias para cometer ataques, mediante la identificación de vulnerabilidades o vacíos de seguridad de los sistemas informáticos.

La privacidad o confidencialidad implica que solamente las personas autorizadas deben leer o acceder a los datos y sistemas específicos. Las exposiciones que hacen los hackers al revelar información de las tarjetas de crédito de los usuarios constituyen un ataque a la confidencialidad. A su vez la integridad significa que sólo las personas autorizadas son capaces de modificar o utilizar los sistemas y también los datos. Los cyberdelincuentes, que mediante técnicas de “hackeo” (*hacking*) logran tener las credenciales de acceso de los usuarios ya sea mediante credenciales de acceso como usuario y contraseña u obteniendo los datos de tarjeta de crédito para hacer una compra fraudulenta, constituye un ataque a la integridad de la información.

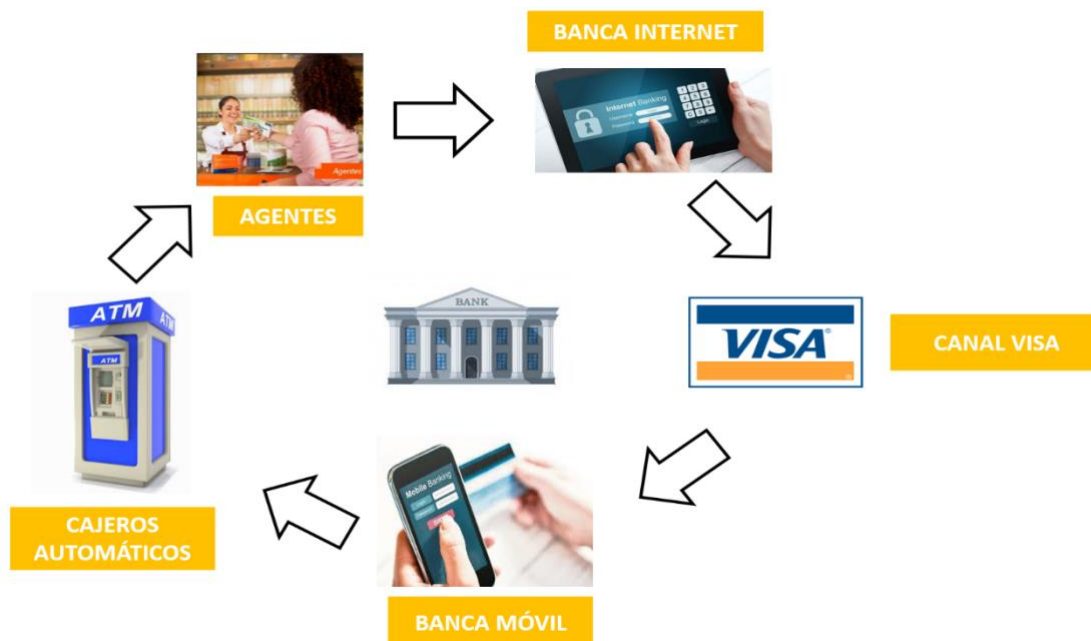
Finalmente, la disponibilidad implica que los usuarios autorizados deben tener acceso a los sistemas y sus datos respectivos en todo momento. Los ataques de Denegación de Servicios (DoS), implica enviar una indeterminada cantidad de solicitudes o peticiones falsas al servidor que administra el sitio web de una empresa, a tal punto de bloquear o ralentizar los accesos de usuarios a dicho sitio web, este evento constituye un ataque a la disponibilidad del servicio. (Crashcourse, 2017).

### **2.3 Banca, canales y transacciones con tarjeta de crédito**

El banco sobre la cual se implementará la solución orientada a la detección del fraude con tarjetas de crédito, brindar los servicios financieros a través de los siguientes canales, tal como se muestra en la Figura 2.2:

**Figura 2.2**

*Canales del banco*



- **Agentes**

Canal donde se realizan operaciones de depósito o retiro con tarjeta presente, implementado en locales de acceso minorista de empresas de diversas industrias como, por ejemplo, farmacias, bodegas, etc.

- **Cajeros automáticos (ATM's)**

Canal ofrecido por el banco para realizar operaciones de retiro de dinero y otras transacciones. Pueden ser de una red administrada por el mismo banco o redes de terceros (ViaBCP, Unibanca, GlobalNet, etc.).

- **Banca Móvil**

Canal mediante el cual el cliente puede realizar operaciones de transferencia de dinero por medio del celular con el uso de una clave dinámica.

- **Banca Internet**

Canal mediante el cual el cliente pueda realizar transferencias de dinero, pago de servicios entre otros, con tarjeta no presente.

- **Canal Visa**

Este canal es ofrecido para todos aquellos clientes que realizan operaciones de compras a través de su tarjeta de crédito y/ o débito. Las transacciones son de dos tipos: tarjeta presente (POS) o tarjeta no presente (compra por internet o compras que no requieran del ingreso de la tarjeta a un terminal).

**Flujo de procesos de una transacción con tarjeta de crédito y/ o débito.**

Roles Principales:

- **ADQUIRIENTE:** Es la institución financiera autorizada por Visa o Procesos MC, que facilita al comercio a cumplir con su obligación de permitir las compras con tarjetas Visa, MasterCard, entre otras marcas, mediante una conexión directa con los bancos emisores de tarjetas.
- **EMISOR:** Es la institución financiera que ofrece el producto de una tarjeta de crédito o débito al usuario.
- **COMERCIO:** Es el establecimiento físico o virtual sobre la cual se hacen las operaciones con tarjetas de crédito o débito, es un canal que permite la interacción del usuario – adquiriente y emisor.

**Figura 2.3**

*Ciclo de una transacción*

## Ciclo de Vida de la Transacción

### Flujo de Proceso de Autorizaciones



Nota. Adaptado de Visa Business School, por Prevención de Fraudes – Manual de participante, 2015, p.10

El flujo de procesos de Autorizaciones de la Figura 2.3 se muestra a continuación:

**Tabla 2.1**

*Flujo de Proceso de Autorizaciones*

Flujo	Descripción
1	El cliente paga con la tarjeta.
2	El comercio digita el monto de la transacción y envía la petición de autorización al adquirente.
3	El adquirente envía electrónicamente la solicitud de autorización por VisaNet(Niubiz).
4	Visa transfiere la petición al Banco emisor de la tarjeta.
5	El banco Emisor valida la cuenta, tarjeta y transacción.
6	El banco Emisor responde inmediatamente con la respuesta a VisaNet(ahora Niubiz)
7	Visa (ahora Niubiz), envía la respuesta del emisor de la Tarjeta del Adquirente
8	El Adquirente envía la respuesta recibida (aprobada o rechazada) al comercio
9	El comercio recibe la respuesta y se completa la transacción

Nota. Incluye todos los procesos para la autorización de una transacción. Adaptado de *Visa Business School*, por Prevención de Fraudes – Manual de participante, 2015, p.10

Respecto al Flujo N°1, el cliente puede pagar con tarjeta presente; es decir, ingresando su tarjeta a un dispositivo POS o con tarjeta No Presente, a través de internet.

Respecto al flujo N°2, Se ingresa los datos personales del cliente (número de la tarjeta, fecha de vencimiento y CVV) para operaciones por internet, lo correspondiente a tarjeta presente, se ingresa la tarjeta al dispositivo POS y se ingresa la clave de 4 dígitos y, posteriormente, se envía la solicitud de autorización adquiriente.

Respecto al flujo N°3, se envía la solicitud de autorización al Banco Emisor de la tarjeta.

Respecto al flujo N°4, El adquiriente transfiere la solicitud al Banco emisor de la tarjeta.

Respecto al flujo N°5, El banco emisor de la tarjeta valida que la información ingresada es correcta (número de la tarjeta, fecha de vencimiento, CVV y clave de 04 dígitos).

Respecto al flujo N°6, Banco emisor de la tarjeta envía la respuesta de validación al Adquiriente, esta puede ser rechazada por varias casuísticas tales como, saldos insuficientes, error del sistema, rechazada por regla de monitoreo o por ser tarjeta con sospecha de fraude.

Respecto al flujo N°7, Visanet envía la respuesta del emisor.

Respecto al flujo N°8, el adquiriente envía la respuesta al comercio (establecimiento físico o medio virtual).

Respecto al flujo N°9, el comercio recibe la información del adquiriente e inmediatamente se procesa la transacción.

#### **2.4 Estadísticas relacionadas a bancos y operaciones con tarjeta de Crédito**

A continuación, se mostrará un gráfico evolutivo del número de transacciones por internet de enero del 2019 hasta junio del 2020, tal como se observa en la tabla 2.2, tabla 2.3 y en la Figura 2.4, la tendencia de crecimiento es notable tanto para aquellas transacciones que se hacen en comercio electrónico internacional, que se refiere a las compras por internet en páginas web administradas dentro del territorio nacional y también la tendencia es evidente con respecto a las operaciones hechas en comercio electrónico local, que básicamente son compras hechas en comercios locales dentro de territorio nacional sea a través de sitios web locales y compras por aplicativos. Por otro lado, a partir de mayo del 2019, las altas de



tarjetas de crédito y débito estaban habilitadas para hacer compras por internet lo que motivó a que el número de transacciones por este canal se incrementara teniendo los picos más altos a partir de febrero del 2020, producto de la pandemia lo que permitió que los clientes hagan compras por internet debido al confinamiento.

**Tabla 2.2**

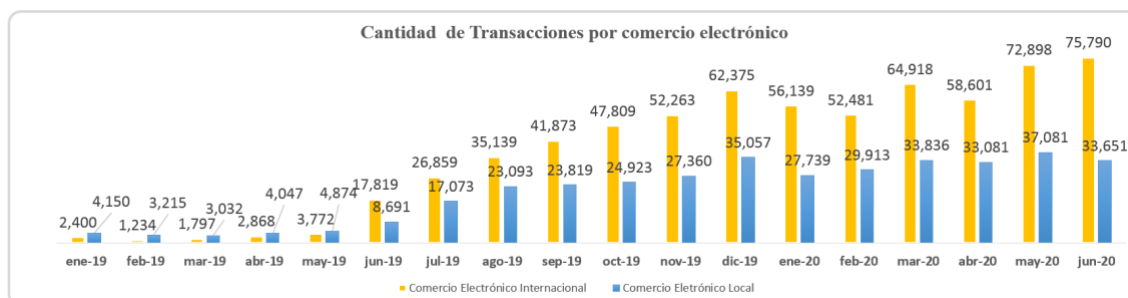
*Evolutivo de transacciones por comercio electrónico (enero 2019 - agosto 2019)*

<b>Tipo</b>	<b>ene-19</b>	<b>feb-19</b>	<b>mar-19</b>	<b>abr-19</b>	<b>may-19</b>	<b>jun-19</b>	<b>jul-19</b>	<b>ago-19</b>
Comercio Electrónico Internacional	2,400	1,234	1,797	2,868	3,772	17,819	26,859	35,139
Comercio Electrónico Local	4,150	3,215	3,032	4,047	4,874	8,691	17,073	23,093
<b>Total</b>	<b>6,550</b>	<b>4,449</b>	<b>4,829</b>	<b>6,915</b>	<b>8,646</b>	<b>26,510</b>	<b>43,932</b>	<b>58,232</b>

**Tabla 2.3**

*Evolutivo de transacciones por comercio electrónico (setiembre 2019 - junio 2020)*

<b>Tipo</b>	<b>sep-19</b>	<b>oct-19</b>	<b>nov-19</b>	<b>dic-19</b>	<b>ene-20</b>	<b>feb-20</b>	<b>mar-20</b>	<b>abr-20</b>	<b>may-20</b>	<b>jun-20</b>
Comercio Electrónico Internacional	41,873	47,809	52,263	62,375	56,139	52,481	64,918	58,601	72,898	75,790
Comercio Electrónico Local	23,819	24,923	27,360	35,057	27,739	29,913	33,836	33,081	37,081	33,651
<b>Total</b>	<b>65,692</b>	<b>72,732</b>	<b>79,623</b>	<b>97,432</b>	<b>83,878</b>	<b>82,394</b>	<b>98,754</b>	<b>91,682</b>	<b>109,979</b>	<b>109,441</b>

**Figura 2.4***Cantidad de transacciones por comercio electrónico*

*Nota.* Incluye los datos de cantidad de transacciones por comercio electrónico. Adaptado de Reportes Internos del Banco Peruano, por Área de Prevención de Fraudes ,2020.

Los importes de transacciones por comercio electrónico se muestran en la tabla 2.4, 2.5 y 2.6. En la figura 2.5 se muestra el evolutivo de importes por comercio electrónico por localidad de enero del 2019 a junio de 2020.

**Tabla 2.4***Importe de transacciones por comercio electrónico (enero 2019 - agosto 2019)*

Tipo	ene-19	feb-19	mar-19	abr-19	may-19	jun-19	jul-19	ago-19
Comercio								
Electrónico	1,722,632	2,303,636	2,768,800	2,630,869	2,759,234	2,883,253	3,606,104	2,310,388
Internacional								
Comercio								
Electrónico	1,060,822	955,549	1,360,043	1,532,551	1,517,458	1,553,679	2,102,009	2,390,602
Local								
<b>Total</b>	<b>2,783,454</b>	<b>3,259,185</b>	<b>4,128,843</b>	<b>4,163,420</b>	<b>4,276,692</b>	<b>4,436,932</b>	<b>5,708,113</b>	<b>4,700,990</b>

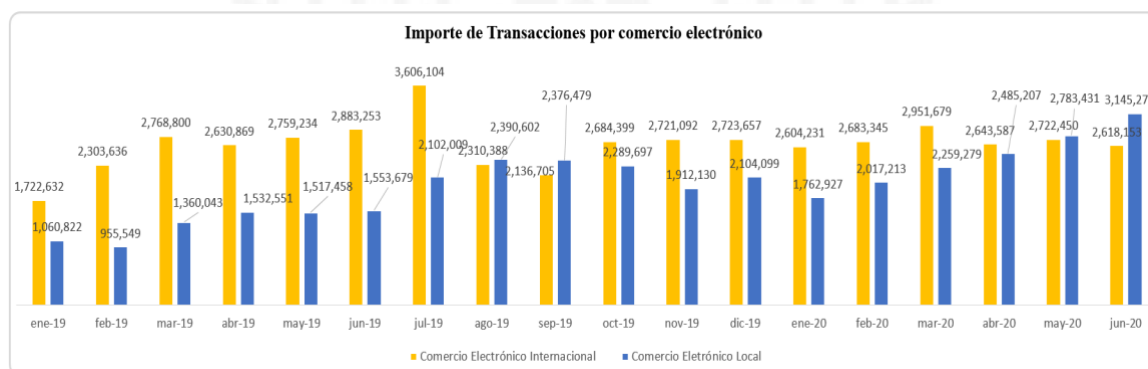
*Nota.* Incluye los datos de cantidad de transacciones por comercio electrónico. Adaptado de Reportes Internos del Banco Peruano, por Área de Prevención de fraudes ,2020.

**Tabla 2.5***Importe de transacciones por comercio electrónico (setiembre 2019 - enero 2020)*

Tipo	sep-19	oct-19	nov-19	dic-19	ene-20
Comercio Electrónico Internacional	2,136,705	2,684,399	2,721,092	2,723,657	2,604,231
Comercio Electrónico Local	2,376,479	2,289,697	1,912,130	2,104,099	1,762,927
<b>Total</b>	<b>4,513,184</b>	<b>4,974,096</b>	<b>4,633,222</b>	<b>4,827,756</b>	<b>4,367,157</b>

**Tabla 2.6***Importe de transacciones por comercio electrónico (febrero 2020 - junio 2020)*

Tipo	feb-20	mar-20	abr-20	may-20	jun-20
Comercio Electrónico Internacional	2,683,345	2,951,679	2,643,587	2,722,450	2,618,153
Comercio Electrónico Local	2,017,213	2,259,279	2,485,207	2,783,431	3,145,277
<b>Total</b>	<b>4,700,558</b>	<b>5,210,958</b>	<b>5,128,794</b>	<b>5,505,882</b>	<b>5,763,431</b>

**Figura 2.5***Importe de Transacciones por comercio electrónico*

*Nota.* Incluye los datos de cantidad de transacciones por comercio electrónico. Adaptado de Reportes Internos del Banco Peruano, por Área de Prevención de Fraudes, 2020.

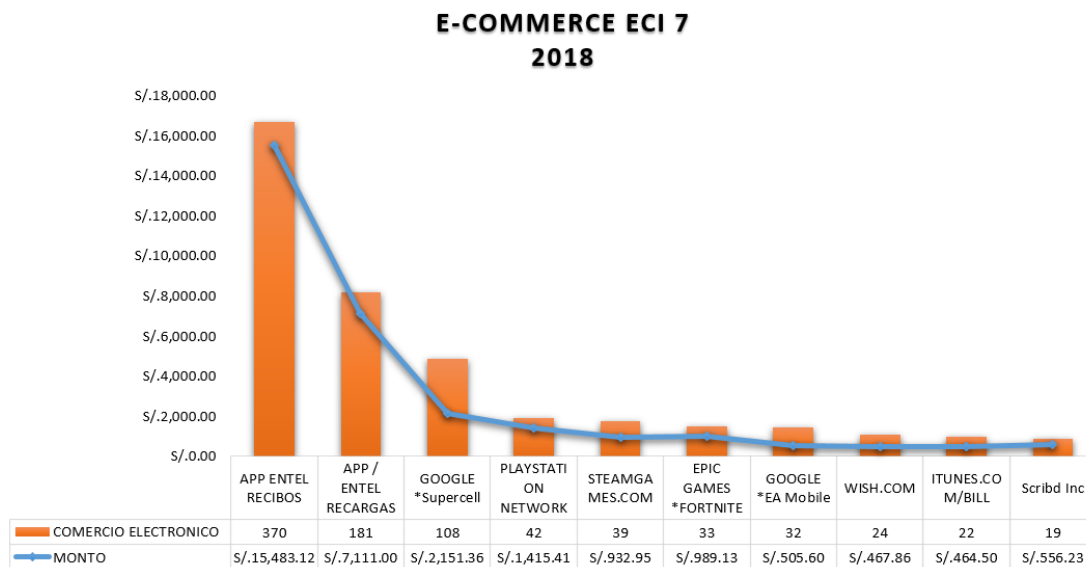
El presente trabajo se enfocará solo en aquellas transacciones realizadas en Internet, tanto en comercios seguros o no seguros. Dentro de la nomenclatura de Visa, las operaciones que se llevan a cabo en internet en comercios no seguros, con tarjeta no

presente, se denominan ECI7, que constituyen transacciones no autenticadas y no seguras, que implica que los comercios no tienen implementado un canal digital seguro, tales como los certificados de seguridad, que garanticen que la información ingresada por el cliente durante una compra está protegida y encriptada. Por el contrario, existen compras por Internet que se realizan los comercios seguro y Visa las identifica como transacciones ECI 5, cuya principal característica radica en que la información ingresada por el tarjetahabiente está protegida y cumple con todos los mecanismos de seguridad como el doble factor de autenticación, que garantiza que la operación sea segura.

El presente gráfico muestra uno de los eventos de fraude que se presentaron durante el primer semestre del año 2018, con respecto a transacciones por internet hechas en comercios No seguros (ECI 7). Es importante mencionar que para poder frenar tales operaciones riesgos, el banco tenía implementado una regla de declinación; sin embargo, el patrón de consumo para este tipo de comercios, que están relacionados a recargas de celular para videojuegos, cambió, y por lo tanto la regla no lo capturó, materializándose el fraude. Posteriormente, luego de un análisis del comportamiento de los clientes para esos comercios se pudo modificar y controlar operaciones en adelante.

**Figura 2.6**

*Transacciones fraudulentas - ECI 7*



*Nota.* Incluye los datos de cantidad de transacciones e importe por comercio electrónico no seguros. Adaptado de Reportes Internos del Banco Peruano- Reportes Fraude ECI 7, por Área de Prevención de Fraudes ,2020.

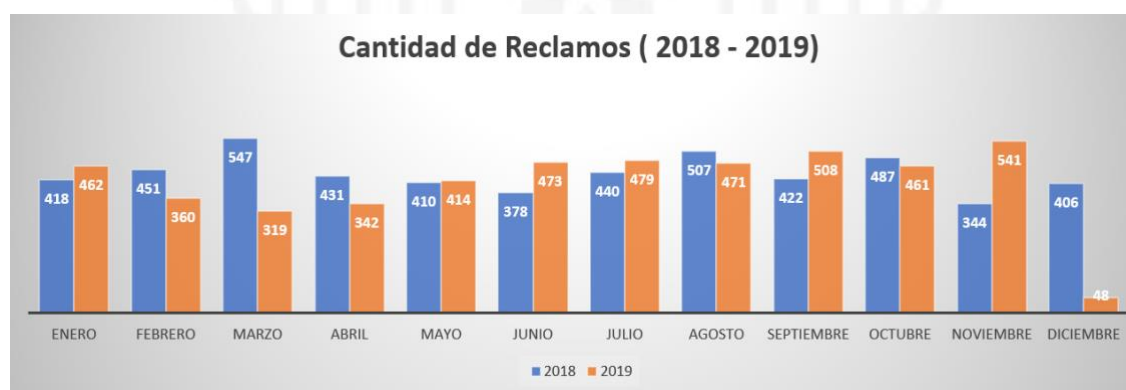
Según el reporte de la División de Investigación de Alta Tecnología (DIVINDAT), durante el año 2019, se registraron 3,012 denuncias de delitos informáticos en el Perú de las cuales los fraudes informáticos y relacionados alcanzaron 2,097, cabe mencionar que sobre este universo 1,641 corresponden a denuncias por transacciones no autorizadas vía internet, 431 casos de compras fraudulentas y finalmente 25 denuncias por caso de clonación de tarjetas de crédito o débito.

Los reclamos a entidades bancarias por casos de consumos no reconocidos han aumentado proporcionalmente al incremento de compras con tarjeta de crédito y / o débito, teniendo mayor concentración sobre aquellas realizadas a través del canal comercio electrónico.

A continuación, se visualiza la cantidad de reclamos por consumos no reconocidos durante el año 2018 y 2019, tal como se puede apreciar en la figura 2.7, la cantidad de reclamos tiene una tendencia de crecimiento por la importante cantidad de fraudes que se concretan.

**Figura 2.7**

*Cantidad de Reclamos (2018-2019)*



*Nota.* Incluye los datos de cantidad de reclamos ingresados por consumos no reconocidos. Adaptado de Reportes Internos del Banco Peruano- Reporte de Reclamos, por Área de Prevención de Fraudes, 2020.

A continuación se muestran las pérdidas brutas de la entidad bancaria por consumos no reconocidos de transacciones fraudulentas del año 2016 al año 2019. Esta información se refiere a la cantidad de dinero que pierde el banco por fraudes bajo distintas

modalidades(phishing, robo, regleta, etc). Cabe mencionar que en la Figura 2.8, se muestran las pérdidas brutas, donde se excluye los montos que se han podido recuperar, producto del contracargo.

### Figura 2.8

*Pérdidas anuales totales*



*Nota.* Incluye los datos de pérdidas en unidades monetarias de fraude del 2016 al 2019. Adaptado de Reportes de SPTF del Banco Peruano, por Área de Prevención de fraudes ,2020.

Durante el desarrollo del presente proyecto, abordaremos temas relacionados a Inteligencia Artificial, algoritmos de aprendizaje automático, así como técnicas de minería de datos para la transformación de nuestra fuente de datos.

### 2.5 Minería de Datos

La minería de datos es el proceso de identificar tendencias y patrones valiosos a partir de grandes volúmenes de datos, combinando diferentes campos de estudio como el aprendizaje automático y estadística, requiriendo la capacidad de analizar y manipular datos. (Adepoju et al., 2019, p. 2).

Bagga et al (2020) sostienen que la minería de datos es una de las técnicas más utilizadas para resolver el problema de detección de fraudes con tarjeta de crédito (p. 104).

## **2.6 Inteligencia Artificial**

### **2.7 Machine Learning**

Adepoju et al. (2019) sostienen que el Aprendizaje Automático es un tipo de inteligencia artificial en las que las computadoras están capacitadas para identificar diseños, dentro de grandes volúmenes de datos para mejorar esos ejemplos de forma natural sin la interceptación del ser humano. (p. 2)

### **2.8 Clasificación de sistemas de Aprendizaje Automático**

#### **Aprendizaje supervisado**

El aprendizaje supervisado es la tarea del Machine Learning que consiste en aprender una función que identifica una entrada a una salida, mediante el ingreso de datos etiquetados con diferentes variables que a través de una formulación matemática genera una función resultante, y que a partir de las variables de entrada pueda predecir una variable de salida.

#### **Aprendizaje no supervisado**

El aprendizaje no supervisado es la tarea del Machine Learning que consiste en inferir una función en relación con ingresos de datos no etiquetados con diferentes variables a través de una formulación matemática, para luego generar una función resultante.

### **2.9 Algoritmos de Machine Learning**

La técnica de minería de datos descriptiva señala las relaciones en los datos o la información y procede a encontrar todas las propiedades y relaciones de los datos sobre la información examinada (Rambola., 2018, p. 1).

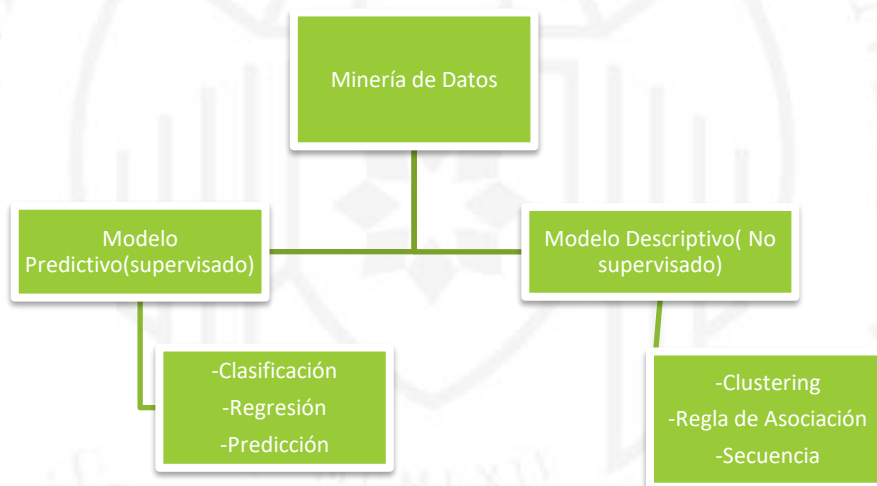
La Inteligencia Artificial es la disciplina que investiga la comprensión e imitación de la inteligencia humana, su tarea principal es construir la teoría del procesamiento inteligente de la información con la inteligencia humana realizada por máquinas inteligentes. (Xian, 2010).

Machine Learning forma parte de la Inteligencia Artificial, que permite, a través del entrenamiento de datos, generar un resultado con grandes volúmenes de datos. Para el tratamiento de los datos se necesitan técnicas estadísticas de minería de datos que conlleven a generar resultados más acertados y con un alto índice de eficiencia y eficacia.

La Figura 2.9 muestra acerca de las técnicas y / o modelos de minería de datos.

**Figura 2.9**

*Técnica y/o modelo Minería de Datos*



*Nota.* La figura representa la estructura de la minería basada en modelos y clasificaciones. Adaptado de Data Mining Techniques for Fraud Detection in Banking Sector, por Rambola et al ,2018, p. 2.

### 2.9.1 Random Forest

Los bosques aleatorios son conjuntos de árboles de decisión aleatorios. Random Forest es uno de los modelos de aprendizaje automático más exitosos para la clasificación y regresión. Combinan muchos árboles de decisión para reducir el riesgo de sobreajuste. (Armel & Zaidouni, 2019, p 4).



Los bosques aleatorios se construyen a partir de un conjunto de datos, utilizando determinadas características y de manera iterativa logrando así la creación de múltiples árboles de decisión ,mediante nodos, a partir de la selección aleatoria de los datos, que van clasificando la información y obteniendo la predicción mediante nuevos casos, cada caso es empujado hacia abajo del árbol y nuevamente clasifica la información bajo cierto criterio y obtiene una ponderación, dicho procedimiento se hace de forma recursiva hasta llegar a los nodos individuales, el nodo que tenga mayor cantidad de condiciones cumplidas por el algoritmo obtendrá la predicción del mismo. (Armel & Zaidouni, 2019, p 4).

Las ventajas del algoritmo Random Forest son:

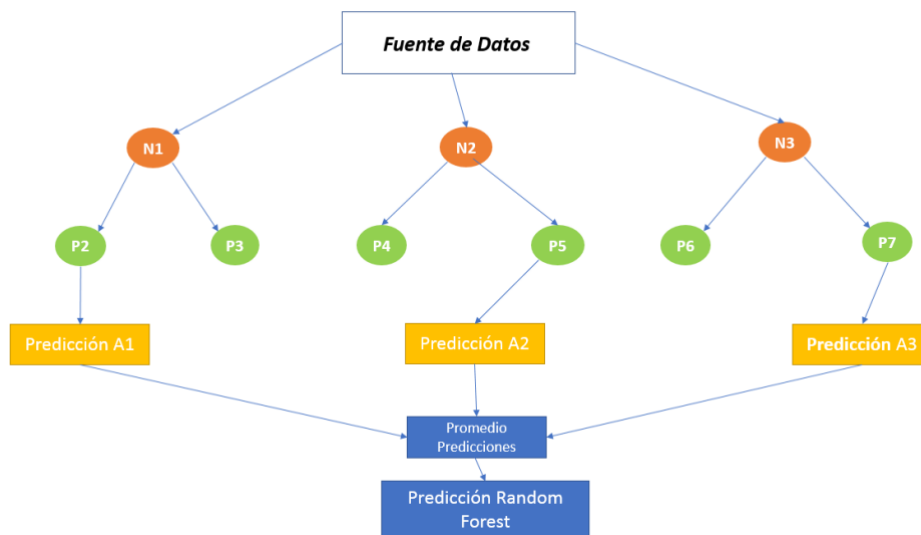
Tipo de método que, en su conjunto, a través de una gran cantidad de datos de entrenamiento, forma un modelo altamente predictivo.

Brinda estimaciones sobre qué variables son importantes en la clasificación.

Alto rendimiento para el manejo de grandes fuentes de datos.

**Figura 2.10**

*Diagrama Random Forest*



*Nota.* Representación gráfica del algoritmo Random Forest. Adaptado de Fraud Detection Using Apache Spark, por Armel & Zaidouni ,2019, p. 5.

## 2.9.2 Regresión Logística

El algoritmo de Regresión Logística usa la función logística y la función sigmoide para realizar una clasificación binaria basada en diversos factores dentro del conjunto de datos. La función sigmoide se usa para encontrar una probabilidad de clasificación binaria. (Adepoju et al., 2019, p. 3).

Representación Matemática de Función Sigmoide:

$$y^i = \frac{1}{1 + e^{-(z)}}$$

$$z = b + m_1x_1 + m_2x_2 + m_3x_3 + \dots + m_nx_n$$

Donde:

y: es la probabilidad de salida

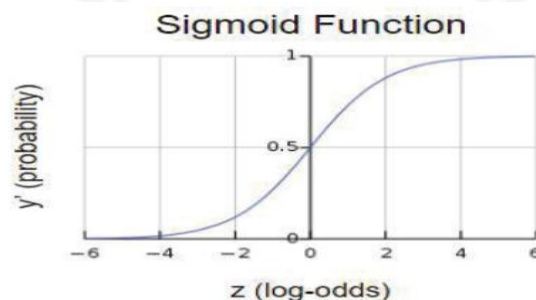
z: es el resultado de las probabilidades de ejemplo

b: es la intersección de la regresión lineal

m: son los valores ponderados

### Figura 2.11

*Función Sigmoide*



*Nota.* Representación gráfica de la función de regresión logística. Adaptado de *Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques* por Adepoju et al., 2019, p. 3.

### **2.9.3 Naive Bayes**

Es un enfoque estadístico que utiliza la mayor probabilidad para tomar decisiones, la probabilidad bayesiana utiliza valores conocidos para estimar probabilidades desconocidas; es decir la lógica y los conocimientos previos se aplican a enunciados que son inciertos. (Bagga et al., 2020, p. 106).

Dicha técnica hace uso del supuesto de independencia condicional entre las características de los datos, las probabilidades condicionales y de las clases de fraude y no fraude se utilizan en el clasificador de Bayes. (Bagga et al., 2020, p. 106).

Ray (2019) señala que el algoritmo Naive Bayes tiene muchas aplicaciones; entre ellas, por ejemplo, sistemas de recomendación, pronóstico de la recaída o progresión del cáncer después de una radioterapia. (p. 38)

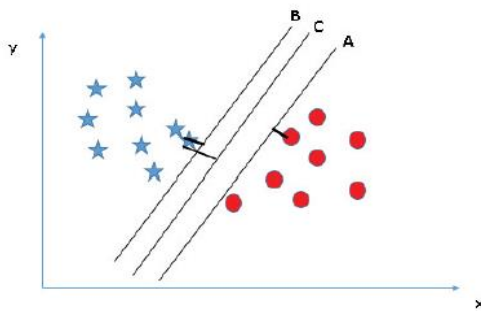
### **2.9.4 Support Vector Machine**

Las Máquinas de Vectores de Soporte son ejemplos de algoritmos supervisados para el aprendizaje supervisado que se aplica a problemas de clasificación y regresión, ya que una máquina de vectores de soporte decidirá la mejor técnica de ajuste para clasificar la información. (Adepoju et al., 2019, p. 4)

En la figura 2.12, se puede ver que los puntos de los datos de la derecha se clasifican como no fraudulentos, mientras que los otros, como fraudulentos. La máquina de vectores de soporte separa la clase a cualquier lado del punto más cercano, dicha distancia se denomina margen y el punto del margen se conoce como vectores de soporte. (Adepoju et al., 2019, p. 4).

## Figura 2.12

### Support Vector Machine



Nota. Representación gráfica del algoritmo de Máquina de Vector de Soporte. Adaptado de *Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques*, por Adepoju et al., 2019, p. 4.

### 2.9.5 K - Means Clustering

Ray (2019) manifiesta que es un algoritmo de aprendizaje no supervisado que se utiliza para resolver problemas de agrupación, siendo una de sus ventajas que es computacionalmente más eficiente que la agrupación jerárquica cuando existe muchas variables (p 38).

El algoritmo K-Means Clustering se puede usar para la clasificación de documentos, segmentación de clientes, análisis de datos de viajes compartidos, agrupación automática de alertas de TI y detección de fraudes sobre seguros. (Ray, 2019, p. 38).

### 2.10 Matriz de confusión

Es un indicador que mide el desempeño completo de modelos, entre ellos, los basados en inteligencia artificial.

Los componentes de la matriz de confusión para la evaluación de los modelos son los siguientes:

- Tasa de Verdadero Positivo.
- Tasa de Verdadero Negativo.

- Tasa de Falso Positivo.
- Tasa de Falso Negativo.

Los verdaderos positivos son clases que se predice que son positivas y las clases verdaderas negativas que se predicen como negativas, pero en realidad son negativas.

Los falsos positivos son clases que se predicen que serán positivas y en realidad son negativas, por su parte los falsos negativos son aquellas clases que se predice que serán negativas cuando en realidad son positivas. (Adepoju et al., 2019, p. 4)

**Figura 2.13**

*Matriz de Confusión*

MATRIZ DE CONFUSIÓN		Predicción	
		Positivos	Negativos
Observación	Positivos	Verdadero Positivo	Falso Negativo
	Negativos	Falso Positivo	Verdadero Negativo

### Métricas de Matriz de Confusión

$$\text{Exactitud: } \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Sensibilidad: } \frac{TP}{TP+FN}$$

$$\text{Precisión: } \frac{TP}{TP+FP}$$

Donde:

TP: True Positive (Verdadero positivo)

FP: False Positive (Falso Positivo)

TN: True Negative (Verdadero negativo)

FN: False Negative (Falso negativo)

## **2.11 Design Thinking**

Es una metodología para la innovación y diseño, usada por los diseñadores para resolver problemas complejos y encontrar soluciones deseables tomando énfasis en la imaginación, lógica, y el razonamiento sistemático para crear ingeniosos resultados en beneficio de los usuarios. (Anand et al., 2015, p. 69)

Design Thinking implica el diseño de actividades cognitivas específicas y consta de cinco pasos o fases que se muestra y detalla a continuación:

### **1. Empatizar**

Fase que tiene como objetivo conocer el público objetivo; es decir, entender sus necesidades, especialmente las físicas y emocionales. El proceso de empatía incluye observar, involucrar y observar al público objetivo. Esta etapa termina con la comprensión del problema. (Anand et al., 2015, p. 69).

### **2. Definir**

Es la segunda fase, que ayuda a crear puntos de vista, proporcionando enfoque del problema identificado, esta fase es muy importante para poder aportar claridad y crear la solución correcta. (Anand et al., 2015, p. 69).

### **3. Idear**

Corresponde a la tercera fase de la metodología, que se dirige a encontrar una amplia gama de posibles soluciones sin mantener las limitaciones de recursos y posibilidades. Siendo una etapa de lluvia de ideas y búsqueda de soluciones creativas. (Anand et al., 2015, p. 69).

#### **4. Prototipar**

Corresponde a la cuarta fase, que involucra la creación de un prototipo de la idea final, dicha etapa inicia con la construcción de los artefactos teniendo en cuenta al usuario final. Esta etapa es importante para la construcción de soluciones. (Anand et al., 2015, p. 69).

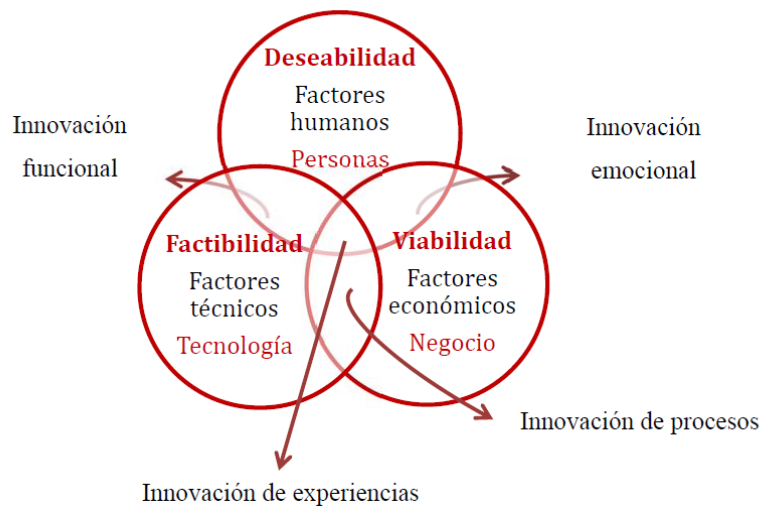
#### **5. Testear**

Corresponde a la etapa final del proceso que implica probar el artefacto creado en la etapa de prototipo, las pruebas se llevan a cabo con el público objetivo. (Anand et al., 2015, p. 69).

Design Thinking, como se indicó anteriormente, corresponde a una metodología innovadora para resolver problemas relacionados a la factibilidad, viabilidad y deseabilidad que presenta una persona. En la figura 2.14 se muestra cómo se relacionan los tres factores que juegan un papel importante en la implementación de dicha metodología.

## Figura 2.14

### Factores Design Thinking



*Nota.* Factores del Design Thinking. Adaptado de *El Design Thinking aplicado en el desarrollo de un Sistema de Información, que permite incrementar la satisfacción de los operarios al reducir los tiempos de atención de Capital Humano*, por Llerena & Terrones, 2018, p. 43.

## 2.12 Componentes de arquitectura de solución

La solución técnica del proyecto se basa en el enfoque de análisis, procesamiento y despliegue de datos a través de una plataforma web basada en la técnica de Machine Learning.

Los componentes tecnológicos que forman parte de la solución son los siguientes:

### APACHE KAKFA

Es una plataforma distribuida de transmisión de datos que permite publicar, almacenar y procesar flujos de registros en tiempo real. Está diseñada para manejar flujos de datos de varias fuentes, constituyéndose una alternativa de mensajería empresarial tradicional ya que al manejar y procesar millones puntos de datos por segundos, lo hace ideal para los desafíos del Big Data.



## SPARK STREAMING

Es una extensión de API principal de Spark que permite el procesamiento de flujos escalables, de alto rendimiento tolerante a fallas de flujo de datos en tiempo real. Los datos pueden ser extraídos de diversas fuentes, como Kafka o Kinesis, los cuales pueden ser procesados por utilizando algoritmos de aprendizaje automático. Estos datos procesados son enviados a un sistema de archivos o bases de datos.

**Figura 2.15**

*Componentes Spark Streaming*



*Nota. Representación gráfica de los componentes de Spark Streaming. Adaptado de Near real time fraud detection with Apache Spark, por Hernández., 2015, p. 15.*

## CASSANDRA SQL

Apache Cassandra es una base de datos NoSQL distribuida basada en un modelo de almacenamiento de “clave-valor”, de código abierto que está escrita en Java. Permite el almacenamiento de grandes cantidades de datos de forma distribuida.

Una de las características más resaltantes de CASSANDRA SQL, se basa en su alto rendimiento en aplicaciones reales debido a elecciones arquitectónicas fundamentales. Además, es altamente escalable ya que permiten implementaciones de producción más grandes y de forma incremental; es decir, que a medida que crezca el volumen de datos, el rendimiento no se verá afectado.

## CONFLUENT CLOUD

Permite la gestión de los servicios en la nube de Apache Kafka, esta plataforma basada en nube permite simplificar la integración y el procesamiento de datos en las nubes de Amazon Web Services, Microsoft Azure y Google Cloud Plataform.

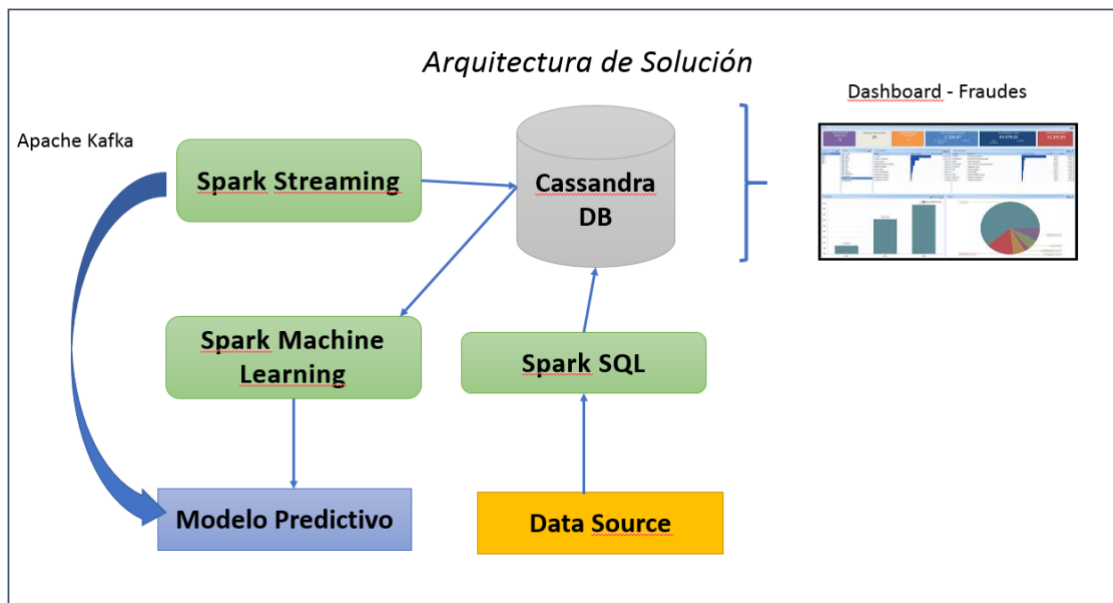
## PYTHON

Es un lenguaje de programación, interpretado, dinámico y multiplataforma, que soporta programación imperativa y programación orientada a objetos.

En la Figura 4.2, se muestra la arquitectura de solución

**Figura 2.16**

*Arquitectura de Solución*



Spark SQL Job importará todos los datos de transacciones del sistema de archivos (fuente de datos) a la base de datos de Cassandra.

Spark Job importará transacciones fraudulentas a la tabla de fraude y aquellas transacciones no fraudulentas a la tabla No- Fraude.

Luego Spark Job leerá las transacciones fraudulentas y no fraudulentas de la base de datos Cassandra. Seguidamente se entrenará sobre estos datos y se creará un modelo, el mismo que se guardará en un archivo del sistema local.

Posteriormente, Streaming Job cargará el modelo desde el sistema de archivos, luego este comenzará a consumir mensajes de transacciones de las tarjetas de crédito desde Apache Kafka. Con este modelo, se detectará si una transacción es un fraude o no. Finalmente se guardarán las predicciones en la base de datos de Cassandra, aquellas transacciones fraudulentas se guardan en la tabla de Fraudes y aquellas transacciones no fraudulentas, en la tabla No Fraude.

Aquí también se automatiza Spark ML Job. Pero en realidad, el equipo de DataScience ejecutará manualmente Spark ML Job. Se ejecutará manualmente una vez a la semana o una vez al mes para crear un nuevo modelo. Se probará la eficiencia del nuevo modelo. Además, se comparará con la eficiencia del modelo anterior. El modelo se irá perfeccionando cuanto mayor data se procese a lo largo del tiempo, esto implica que el nivel de certeza de detección de fraudes será óptimo.

### **2.13 Metodología Ágiles**

La metodología sobre la cual se llevará la ejecución del proyecto, corresponde al marco ágil de SCRUM que abarca los siguientes elementos:

- **Product Backlog**

Corresponde a la lista de actividades pendientes a desarrollar; constituye una serie de tareas constituidas por historias de usuarios y estas se deben ordenar en función a la prioridad que implica para el desarrollo del proyecto.

- **Sprint Planning**

Corresponde a las reuniones que se llevan a cabo al inicio de cada Sprint donde participa el equipo del proyecto, y donde se discute el desarrollo de actividades correspondiente al Backlog del producto.

- **Sprint Backlog**

Corresponde a la lista de pendientes del Sprint e implica saber el cómo se va a desarrollar el Sprint, en la cual se identifica una o más tareas por historia de usuario, las cuales son agrupadas en un Sprint Backlog y finalmente son derivadas a los miembros del equipo de desarrollo.

- Daily Scrum

Son reuniones diarias que lleva a cabo el equipo SCRUM a fin de saber las actividades que se realizaron el día previo, lo que se hará en el día y cuáles fueron aquellos impedimentos o restricciones que no permitieron lograr el objetivo. Estas reuniones no tienen una duración de más de 15 minutos.

- Sprint Review

El Product Owner explica qué ítems del Product Backlog han sido finalizados y cuales quedan pendiente de entrega y sobre ello se define cual es el siguiente que se realizará.



## CAPÍTULO III: FUNDAMENTACIÓN DEL PROYECTO

### 3.1 Fundamentación de la deseabilidad del proyecto

La prevención del fraude es uno de los mayores retos que tienen las organizaciones en todo el mundo, independientemente del giro del negocio, los fraudes pueden materializarse de diversas maneras.

Según un estudio realizado por la Cámara Peruana de Comercio Electrónico (CAPECE, 2019, sección de Prensa, párr.2), nuestro país ocupa el sexto lugar en Latinoamérica en referencia al volumen de transacciones realizadas por internet, que registró un crecimiento del 31%, que expresado en unidades monetarias representa US\$ 4 mil millones durante el 2019.

Por otro lado, los daños causados por evento de fraudes en el pago electrónico en todo el mundo, ha alcanzado \$7,6 mil billones en el 2010 a \$ 21,81 mil millones en el 2015, representando un aumento del 300% en 5 años (Zamini & Gholamali Montazer, 2018).

El fraude financiero podría ser una preocupación creciente con la forma de alcanzar consecuencias dentro de las organizaciones de la empresa y el comercio financiero. (Rambola, Prateek Varshney, & Prashant Vishwakarma, 2018).

El confinamiento impuesto por el COVID-19 en varios países, ha provocado que centros de monitoreo de seguridad en áreas afectadas hayan cerrado, comprometiendo la seguridad de varias compañías. Este es el escenario ideal para que los defraudadores perpetren sus ataques y comprometan la seguridad de los datos confidenciales, así como la continuidad operativa de las organizaciones.

El impacto que implica no contar con los recursos suficientes para hacer gestiones en el monitoreo de transacciones y seguridad es significativo, ya que al cerrar sus operaciones debido a la crisis económica mundial y frente a los grandes volúmenes de transacciones no son capaces de prevenir los ataques y nuevas modalidades de fraude. En el caso de Perú, los casos de fraudes con mayor impacto son los relacionados a phishing.

Sobre el enfoque orientado a quienes va dirigido este proyecto, se busca satisfacer la necesidad de poder disminuir la carga de trabajo por partes de los analistas de reclamos de fraude, debido a la gran cantidad de estos. También busca atender las frustraciones por parte del consumidor, ya que identifica el fraude luego de la emisión de su estado de cuenta; no de manera inmediata. Esto origina un congestionamiento de las líneas telefónicas y por ende una mayor carga de trabajo por parte de los agentes de monitoreo, quienes establecen comunicación telefónica.

La cantidad de transacciones por internet se han incrementado según se ha indicado anteriormente; sin embargo, con la llegada de la pandemia del COVID-19, el comportamiento del consumidor en el Perú ha cambiado debido al aislamiento social, en la que comprar productos o realizar pagos en comercios electrónicos se ha visto una necesidad, por lo que los niveles de inseguridad y desconfianza por parte del consumidor ha ido disminuyendo.

El proceso de compras por internet maneja un flujo simple y rápido, cuando una persona quiere realizar una compra por internet, ya sea para comprar un electrodoméstico, comprar boletos de avión o reservar un taxi, lo hace a través de un equipo celular o una computadora conectada a Internet. Así como en el ambiente físico existen establecimientos seguros, ya sea porque existen componentes que garanticen dicha seguridad, también existen establecimientos físicos no seguros para los que se tiene desconfianza por los pocos mecanismos de seguridad que puede involucrar una compra. Lo mismo sucede en el ambiente online, en donde existen comercios seguros y no seguros. La compra en un comercio no seguro tiene mayor riesgo dado que los datos no son encriptados ni cumplen con los niveles mínimos de seguridad, por lo que la información del usuario puede ser expuesta a cualquier persona; muy por el contrario, sucede en establecimientos seguros, en donde la información del cliente y los datos de la tarjeta es cifrada y resguardada.

El usuario, siempre está expuesto a numerosos riesgos; por ejemplo pérdida de su tarjeta de crédito, robo del celular, entre otros, tales escenarios significan una oportunidad para el defraudador y concretar compras fraudulentas, ya que en algunas plataformas de pago, los datos que se pide para la compra son el número de la tarjeta, CVV y fecha de vencimiento, datos que se encuentran físicamente en la tarjeta o pueden ser visualizados a través de la aplicación móvil del banco; en caso el usuario hay sido víctima de robo o ataque de phishing y son dos datos mínimos necesarios que se utilizan para poder concretar una

compra online, por ello es de vital importancia que el comprador tenga una cultura orientada a la prevención del fraude.

### **3.2 Fundamentación de la factibilidad del proyecto**

Actualmente en el mercado existen ya soluciones integrales basadas en la prevención de fraudes en operaciones de banca digital y web, que tiene como objetivo reducir las pérdidas de las organizaciones afectadas por los fraudes, buscar mejorar la experiencia del cliente y disminuir la desconfianza del consumidor antes de hacer una compra.

En el mercado existe numerosas soluciones por parte de los líderes de medios de pago y empresas que se dedican a diseñar e implementar soluciones de fraude; sin embargo, estas soluciones son estáticas pues se basan en reglas; es decir, en construir una expresión lógica basada en varios parámetros que, de cumplir dicha condición, declinan la transacción. La situación actual, y sobre todo con el avance de las nuevas tecnologías y la extensión de canales que han migrado a lo digital, ha permitido que el patrón del consumidor cambie y sea dinámico en el tiempo. Esta situación implica redefinir constantemente las reglas implementadas, lo que no constituye una forma eficiente de la gestión de fraude financiero. La solución que se propone está basada Machine Learning, que, mediante algoritmos de aprendizaje automático, logra que las transacciones fraudulentas puedan ser detectadas teniendo en consideración la habitualidad del tarjetahabiente, puesto que, ante cualquier, caso atípico, ya sea porque el cliente hace un consumo que está fuera de su patrón o quizás el consumo se hace a través de un canal no frecuente con un importe muy alto.

#### **Monitor Plus DBFD**

Es una solución integral para prevenir el fraude externo e interno en transacciones de alto riesgo. En el mercado peruano existen muchas instituciones que han adoptado dicha solución para poder prevenir el fraude. Su solución está basada en 05 capas:

- Análisis relacional.
- Análisis multicanal.
- Monitoreo de Canal.
- Análisis de comportamiento durante la sesión.
- End Point.

## Paytrue

Es una solución tecnológica para la administración de medios de pago y la prevención de fraudes transaccionales; sus soluciones atienden los requerimientos de bancos, instituciones financieras, empresas *retail*, entre otros.

Dicha solución también permite la creación de reglas de declinación en tiempo real y alertamiento.

## Modelo Canvas

Es muy importante conocer y entender cómo este proyecto beneficiará a los involucrados y cuál es la propuesta de negocio, por ello se ha diseñado el Modelo Lienzo de Negocios (Business Model Canvas), que permite identificar con mayor claridad y detalle hacia donde está dirigido el proyecto y cuál es la propuesta. En la figura 3.1 se muestra el Lienzo Model Canvas.

**Figura 3.1**

*Lienzo Model Canvas*

<b>Business Model Canvas</b>				
<b>Socios clave</b>	<b>Actividades clave</b>	<b>Propuestas de valor</b>	<b>Relación con clientes</b>	<b>Segmentos de clientes</b>
Consultores Externos. Stakeholders. Especialistas en soluciones tecnológicas. Proveedores dedicados a brindar soluciones en prevención de fraudes.	Machine Learning. Análisis de Datos. Inteligencia Artificial. Algoritmos de Aprendizaje. <b>Recursos clave</b> Desarrolladores. Analistas de base de datos. Especialistas tecnología Cloud.	Brindar al analista, una plataforma confiable y efectiva para detectar casos de fraude.  Disminuir el exceso de tareas adicionales como análisis de datos.	Sesiones de asesoramiento. Soporte técnico especializado.  <b>Canales</b>  Plataforma web	Instituciones financieras.  Analista y/o especialistas en prevención de fraude.
<b>Estructura de costos</b> Pago a desarrolladores, analistas y especialistas		<b>Fuente de ingresos</b> Pago único por la plataforma		



## **Propuesta de Valor**

La propuesta de valor es brindar al analista de fraudes una herramienta amigable y entendible, que permita detectar y prevenir el fraude financiero realizados en compras por Internet, que facilite el control mediante indicadores de gestión que ofrece la plataforma basada en Machine Learning.

## **Canales**

Los canales que permitan dar a conocer la solución, son los relacionados al sector de entidades financieras (bancos, cajas municipales, financieras, entre otros), mediante alianzas con socios estratégicos, asistencia a eventos relacionados a la prevención del fraude financiero, charla o seminarios relacionadas a la Gestión del Riesgo Operacional organizados anualmente por ASBANC, a fin de dar a conocer esta solución basada en inteligencia artificial y los beneficios que esto trae a las organizaciones que la implementan.

## **Ingresos**

Los ingresos están relacionados al costo total por la solución y una comisión sujeta a una tasa de éxito por aquellas transacciones detectadas y declinadas oportunamente por fraude.

## **Actividades Clave**

Las actividades clave corresponden a las tareas de los involucrados en el proyecto tales como diseño del modelo analítico, análisis de datos, aplicación de técnicas estadísticas, procesos involucrados en una solución que se basa en Machine Learning.

## **Recursos Clave**

Los recursos claves comprenden al personal que estará a cargo de la solución técnica del proyecto como se muestra a continuación:

- Científico de Datos.
- Experto en Soluciones Cloud.
- Analista Programador.
- Analista de Base de Datos.

Los recursos no solamente contemplan personas, sino también recursos de hardware tales como laptops. Además de recursos de software como plataformas para la construcción del código fuente de la solución y recursos *cloud* para el despliegue de la solución y su puesta en marcha.

### **Alianzas Clave**

Los socios clave del proyecto, son los especialistas en prevención de fraudes, empresas líderes en soluciones basadas en inteligencia artificial y motores de fraudes.

### **Estructura de Costos**

Los costos se derivan, básicamente, del pago al personal especializado que juega un papel clave en el desarrollo de la solución. Además, se debe considerar los costos de servicios *Cloud* y recursos necesarios para el aprendizaje.

## **3.3 Fundamentos de la Viabilidad**

### **3.3.1 Pérdidas económicas del banco con relación al fraude**

A continuación, se muestra un cuadro resumen por año de las pérdidas y montos recuperados, así como la tasa de recupero de los fraudes realizados producto de un reclamo.

Los montos recuperados corresponden a los reclamos presentados por el cliente con casos confirmados de fraudes, que, bajo el análisis de analista de reclamos, fue declarado como improcedente y el monto de las transacciones fue recuperado por el banco. Este

escenario corresponde a transacciones de los diferentes canales del banco materia del presente trabajo.

En la tabla 3.1, se visualiza que, ante la gran cantidad de pérdidas económicas, en todos los canales del banco peruano, por fraude, solamente se recupera el 8.75%, lo que implica una tasa de recuperio baja.

**Tabla 3.1**

*Monto monetario recuperado y perdido*

<b>Año</b>	<b>Monto Perdido</b>	<b>Monto Recuperado</b>	<b>Tasa Recuperio</b>
2016	S/ 2,211,886.55	S/ 163,021.33	7.37%
2017	S/ 2,930,578.80	S/ 394,063.00	13.45%
2018	S/ 1,634,251.99	S/ 110,506.23	6.76%
2019	S/ 1,627,983.73	S/ 146,859.81	9.02%

Lo correspondiente al canal de comercio electrónico o compras por Internet, las pérdidas por fraude correspondiente al 2018 y 2019 se muestra en la Tabla 3.2:

**Tabla 3.2**

*Pérdidas monetaria por comercio electrónico*

<b>Descripción</b>	<b>2018</b>	<b>2019</b>
Pérdidas por fraude – Internet	S/ 128,372.30	S/ 142,50376

Para aquellas operaciones fraudulentas hechas por internet, existen tipos de operaciones.

- Compras con Segundo factor de autenticación:
  - ✓ Son aquellas operaciones en la cual el usuario realiza la compra por Internet y cuenta con dos factores de autenticación, uno de estos es Verified by Visa, mediante el cual se envía un código dinámico mediante un mensaje de texto SMS al celular del usuario.
- Compras realizadas con CVV2 y Fecha de vencimiento:

- ✓ Son aquellas operaciones, en las que la tarjeta habiente ingresa los datos del número de la tarjeta, CVV2 y fecha de vencimiento para hacer efectiva la compra. En este tipo de operaciones, el comercio es quién asume el riesgo de la compra.

Los procesos de contracargo se producen cuando un cliente reclama por una operación no reconocida con su tarjeta, luego el Banco, a través de la gestión del analista de reclamos, genera una solicitud de contracargo al comercio correspondiente. Posteriormente el comercio envía las justificaciones acerca de las compras hechas, luego el banco emisor recibe los sustentos respectivos por parte del comercio. Si la solicitud de contracargo es denegada y validada tanto por el banco emisor como el comercio, aduciendo que la compra no se hizo de manera correcta y legítima dado que se cumplieron con los procesos establecidos, el comercio es quien asume la totalidad del importe por la compra, caso contrario quien asume el importe es el banco, constituyéndose una pérdida.

### **3.3.2 Flujo de Caja**

Para identificar los beneficios económicos y el retorno de la inversión de este proyecto, se debe identificar los costos asociados.

Los análisis de costo-beneficio ayudan rápidamente a determinar si los beneficios generales de la solución basada en machine Learning superan los costos incurridos para su implementación.

Las pérdidas económicas por fraudes hechos por compras por Internet durante el año 2018 fueron de S/. 128,372.30 y durante el año 2019 ascendieron a S/. 142,503.76, un incremento del 11%.

Los beneficios obtenidos por el desarrollo de la solución permitirán reducir las futuras pérdidas monetarias por fraudes. Según los expertos las soluciones basadas en Machine Learning permiten reducir hasta un 40-50% las pérdidas monetarias; sin embargo, al adoptar esta nueva solución y teniendo en consideración que el modelo necesita de una determinada cantidad de datos y tiempo para entrenar y detectar los fraudes, se ha asumido que, en una primera instancia, con la solución, se podrá reducir el 35% de las pérdidas económicas.

Para el desarrollo del flujo de caja se consideró datos pronosticados de pérdidas por fraude de agosto del 2020 hasta diciembre del 2020 considerando una tasa de crecimiento del 11%, la que constituye la misma tasa de incremento del periodo 2019 con respecto al periodo 2018.

El proyecto iniciará en agosto del 2020 y tendrá una duración de implementación de 04 meses, es por ello por lo que, a inicios de diciembre del 2020, se empezarán a ver los resultados de la inversión para reducir las pérdidas económicas por fraude. A partir de diciembre del 2020 se hizo el cálculo del Valor Actual Neto y se obtuvo un total de S/ 139,876.72 a una tasa de descuento del 15%, que constituye una proporción estándar que se utiliza para proyectos de Machine Learning orientado a soluciones de prevención de fraudes, siendo el VAN un valor positivo, implica que el proyecto es económicamente viable y se recuperará el monto invertido en el mes de diciembre enero del 2022.

**Tabla 3.3**

*Retorno de inversión (agosto 2020 - diciembre 2020)*

Descripción	ago-20	sep-20	oct-20	nov-20	dic-20
Pérdidas fraude internet	S/ 17,600.00	S/ 15,075.75	S/ 11,077.85	S/ 10,406.42	S/ 18,416.29
Pérdidas evitadas por la solución	S/ 6,160.00	S/ 5,276.51	S/ 3,877.25	S/ 3,642.25	S/ 6,445.70
Fraudes no deducibles	S/ 11,440.00	S/ 9,799.24	S/ 7,200.60	S/ 6,764.17	S/ 11,970.59
Costo Cloud + Mantenimiento					-S/ 101,507.72
Beneficios de solución					S/ 107,953.42

**Tabla 3.4**

*Flujo de caja (enero 2021 - mayo 2021)*

Descripción	ene-21	feb-21	mar-21	abr-21	may-21
Pérdidas fraude internet	S/ 43,691.65	S/ 17,381.90	S/ 15,489.43	S/ 18,528.73	S/ 8,553.54
Pérdidas evitadas por la solución	S/ 15,292.08	S/ 6,083.67	S/ 5,421.30	S/ 6,485.06	S/ 2,993.74
Fraudes no deducibles	S/ 28,399.57	S/ 11,298.24	S/ 10,068.13	S/ 12,043.68	S/ 5,559.80
Costo Cloud + Mantenimiento	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72
Beneficios de solución	S/ 15,999.79	S/ 6,791.38	S/ 6,129.02	S/ 7,192.77	S/ 3,701.46

**Tabla 3.5***Flujo de caja (junio 2021 - octubre 2021)*

<b>Descripción</b>	<b>jun-21</b>	<b>jul-21</b>	<b>ago-21</b>	<b>sep-21</b>	<b>oct-21</b>
Pérdidas fraude internet	S/ 21,066.39	S/ 26,352.77	S/ 19,360.00	S/ 16,583.33	S/ 12,185.63
Pérdidas evitadas por la solución	S/ 7,373.24	S/ 9,223.47	S/ 6,776.00	S/ 5,804.16	S/ 4,264.97
Fraudes no deducibles	S/ 13,693.15	S/ 17,129.30	S/ 12,584.00	S/ 10,779.16	S/ 7,920.66
Costo Cloud + Mantenimiento	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72
Beneficios de solución	S/ 8,080.95	S/ 9,931.19	S/ 7,483.72	S/ 6,511.88	S/ 4,972.69

**Tabla 3.6***Flujo de caja (noviembre 2021 - marzo 2022)*

<b>Descripción</b>	<b>nov-21</b>	<b>dic-21</b>	<b>ene-22</b>	<b>feb-22</b>	<b>mar-22</b>
Pérdidas fraude internet	S/ 11,447.06	S/ 20,257.91	S/ 45,876.23	S/ 18,251.00	S/ 16,263.90
Pérdidas evitadas por la solución	S/ 4,006.47	S/ 7,090.27	S/ 16,056.68	S/ 6,387.85	S/ 5,692.36
Fraudes no deducibles	S/ 7,440.59	S/ 13,167.64	S/ 29,819.55	S/ 11,863.15	S/ 10,571.53
Costo Cloud + Mantenimiento	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72
Beneficios de solución	S/ 4,714.19	S/ 7,797.99	S/ 16,764.40	S/ 7,095.57	S/ 6,400.08

**Tabla 3.7***Flujo de caja (abril 2022 - agosto 2022)*

<b>Descripción</b>	<b>abr-22</b>	<b>may-22</b>	<b>jun-22</b>	<b>jul-22</b>	<b>ago-22</b>
Pérdidas fraude internet	S/ 19,455.17	S/ 8,981.22	S/ 22,119.71	S/ 27,670.41	S/ 20,328.00
Pérdidas evitadas por la solución	S/ 6,809.31	S/ 3,143.43	S/ 7,741.90	S/ 9,684.64	S/ 7,114.80
Fraudes no deducibles	S/ 12,645.86	S/ 5,837.79	S/ 14,377.81	S/ 17,985.77	S/ 13,213.20
Costo Cloud + Mantenimiento	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72
Beneficios de solución	S/ 7,517.03	S/ 3,851.14	S/ 8,449.62	S/ 10,392.36	S/ 7,822.52

**Tabla 3.8***Flujo de caja (setiembre 2022 - diciembre 2022)*

<b>Descripción</b>	<b>sep-22</b>	<b>oct-22</b>	<b>nov-22</b>	<b>dic-22</b>
Pérdidas fraude internet	S/ 17,412.49	S/ 12,794.91	S/ 12,019.41	S/ 21,270.81
Pérdidas evitadas por la solución	S/ 6,094.37	S/ 4,478.22	S/ 4,206.79	S/ 7,444.78
Fraudes no deducibles	S/ 11,318.12	S/ 8,316.69	S/ 7,812.62	S/ 13,826.03
Costo Cloud + Mantenimiento	-S/ 707.72	-S/ 707.72	-S/ 707.72	-S/ 707.72
Beneficios de solución	S/ 6,802.09	S/ 5,185.94	S/ 4,914.51	S/ 8,152.50



## CAPÍTULO IV: DEFINICIÓN DEL PROYECTO

### 4.1 Definición del proyecto

El alcance inicial del presente proyecto es proporcionar una plataforma web basada en inteligencia artificial utilizando el algoritmo Random Forest, que permita detectar el fraude por Internet a través de la visualización de las transacciones identificadas como potencialmente fraudulentas. Además, el sistema, mediante una cuenta administrador, permitirá la creación de usuarios para que el personal del banco pueda gestionar dichas alertas de fraude. Asimismo, mostrará la eficiencia de las alertas desplegadas en el sistema web atendidas por usuario, esto permitirá al analista de fraudes tener un control sobre el rendimiento de cada agente de monitoreo y las cantidades de alertas que atienden. Dicho sistema mostrará en tiempo real todas las transacciones posibles de fraude para su posterior gestión por parte del analista de monitoreo. La solución tecnológica basada en Aprendizaje Automático implementará el algoritmo Random Forest para que, a través del entrenamiento de los datos proporcionados, permita la generación del modelo predictivo. La ejecución periódica de entrenamiento de los nuevos datos permitirá obtener un modelo predictivo más inteligente que permita detectar los fraudes por comercio electrónico con un alto índice de confiabilidad y eficiencia.

#### 4.1.1 Aliviadores de frustraciones y creadores de alegría

El Lienzo de la Propuesta de Valor se define como un método visual integrado por tres elementos: el mapa de valor, que describe de manera estructurada y detallada las características de una propuesta de valor del caso de negocio. A su vez conformado por el perfil del cliente, donde se describe de manera detallada el segmento de cliente del modelo de negocio. Finalmente, el encaje, que determina la coincidencia o *match* del perfil del cliente con el mapa de valor propuesto.

El método en mención se utilizó para identificar las actividades que los usuarios están realizando y cuál es la percepción de estos con respecto a las tareas que realizan, esto involucra determinar sus quejas o frustraciones para, luego, proponer mejoras que ayuden

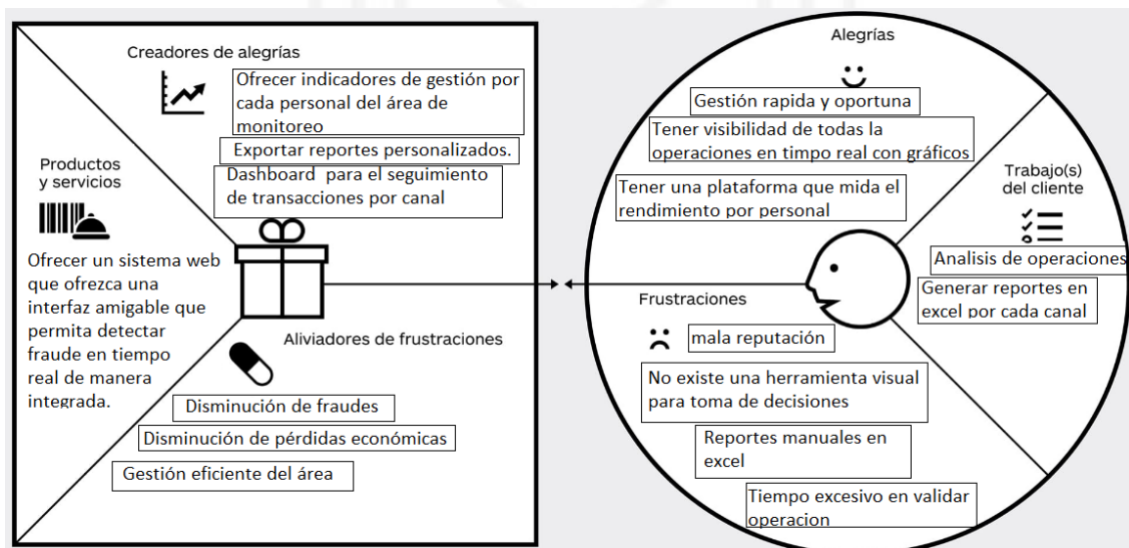


a disminuir el sentir del usuario final. Para llevar a cabo la elaboración del Lienzo se formularon preguntas al analista de fraudes, esto se detalla en la tabla 5.1.

Como se puede observar en la figura, al analizar las alegrías, los trabajos del cliente y los puntos de dolor, se pudo llegar a la conclusión de que existe un problema general con respecto a la eficiencia del actual sistema que gestionan para la prevención del fraude. Los usuarios que usan actualmente la plataforma tienen frustraciones, ya que el sistema no tiene una interfaz de usuario para ver la información del cliente de manera centralizada, sino que el usuario hace múltiples búsquedas para la validación de la transacción; esta situación genera demoras y una gestión ineficiente. Por otro lado, los usuarios que usan el sistema hacen reportes manuales en Excel, que en muchas ocasiones tienen errores, lo que perjudica los datos para la generación de indicadores. Es por ello que, sobre la base de lo que genera frustraciones se ha identificado la necesidad de poder ofrecer una gestión eficiente y oportuna de los fraudes por comercio electrónico basado en un sistema web que detecte transacciones fraudulentas y que ofrezca adicionalmente un menú con reportes y el status de las transacciones en tiempo real.

**Figura 4.1**

*Lienzo propuesta de valor*



## **4.2 Objetivos del proyecto**

### **4.3 Objetivo general**

Apoyar al analista de fraudes a través de una plataforma web confiable, que permita detectar de manera oportuna los casos de fraudes en tiempo real, basado en inteligencia artificial.

#### **4.3.1 Objetivos específicos**

- Identificar las variables más relevantes del modelo predictivo.
- Manejo y tratamiento de datos mediante técnicas de minería de datos.
- Desarrollar el algoritmo Random Forest que genere predicciones de fraude.

### **4.4 Beneficios esperados**

- Incremento de la reputación del área de Prevención de fraudes a nivel interno.
- Entendimiento a cabalidad del analista de la situación actual del área mediante la visualización de los reportes en el Sistema web.
- Supervisión y control de los agentes de monitoreo mediante indicadores de gestión a través de una sola plataforma.
- Apoyo y retroalimentación a los agentes de monitoreo sobre las transacciones etiquetadas como fraudes por la herramienta para correspondiente gestión.
- Reducción de las pérdidas económicas por fraude.
- Mejoramiento de la experiencia del cliente mediante una atención oportuna.
- Disminución de los reclamos por consumos no reconocidos.

#### **4.4.1 Costos totales del proyecto**

Los costos del proyecto involucran los pagos al personal que estará a cargo de la solución.

El científico de datos tendrá un costo de S/8,000 mensuales, el analista programador, por su parte, S/5,500 mensuales, el experto en plataformas cloud, S/4,500 mensuales.

El analista de base de datos incurrirá en un costo mensual de S/3,200 y el personal a cargo de velar por el cumplimiento de la metodología ágil, tendrá un costo de S/ 4,000 mensuales. Es importante recalcar que el proyecto tendrá una duración de cuatro meses por lo que el costo total constituirá una suma de S/101,507.72, que incluye un costo por recursos de la plataforma Confluent Cloud para el despliegue de la solución por S/707.72 mensuales.

**Tabla 4.1**

*Costo de la solución*

<b>Descripción</b>	<b>Costo mensual</b>	<b>Costo Total</b>
Científico de Datos	S/ 8,000.00	S/ 32,000.00
Analista programador	S/ 5,500.00	S/ 22,000.00
Experto Soluciones Cloud	S/ 4,500.00	S/ 18,000.00
Analista Base de Datos	S/ 3,200.00	S/ 12,800.00
Agile Coach	S/ 4,000.00	S/ 16,000.00
Coste Cloud	S/ 707.72	S/ 707.72
<b>Costo Total de Solución</b>		<b>S/ 101,507.72</b>

#### **4.5 Segmento de Mercado**

Los usuarios interesados en la solución planteada, justificada en una herramienta tecnológica web, son las siguientes:

- **Gerente de Riesgo Operacional**, tiene gran preocupación que los índices de fraudes son altos y que, si bien tiene una herramienta que permite declinar y alertar operaciones fraudulentas mediante reglas de monitoreo, estas no son actualizadas de manera oportuna.
- **Analista de fraudes**, es el rol que analiza la información y en función a un análisis del comportamiento del consumidor puede mejorar el rendimiento de las reglas que; sin embargo, no se hace de manera oportuna. La solución que, actualmente, tiene el banco, para la gestión de declinación y alertamiento de operaciones, mediante creación de reglas, no permite

exportar data histórica en gran volumen, motivo por el cual el análisis de la información es limitado y no permite la implementación de reglas efectivas para evitar los casos de fraudes.

- **Analista de reclamos**, recibe muchos reclamos por casos de fraudes por Internet, y tardan mucho tiempo en dar respuesta a los reclamos, ya que buscan información desde numerosas fuentes para validar las transacciones, generando retraso en la gestión. Con la solución podrá reducir su carga de trabajo, mediante el acceso a una plataforma web donde pueda visualizarse toda la información del cliente y los detalles de la operación, a fin de disminuir los tiempos de resolución.
- **Analista de monitoreo de alertas**, la solución permitirá una mayor eficiencia en el desempeño de su trabajo, puesto que, a través, que la solución permitirá una disminución de llamadas telefónicas a los clientes para validar sus operaciones.
- **Jefe de monitoreo de alertas**, gestionará las actividades junto con el equipo de monitoreo y consolida la información de transacciones fraudulentas por agente de monitoreo en archivos Excel, a partir de lo cual se mide la productividad del agente mediante la cantidad de llamadas que ha recibido y/o gestionado al cliente para hacer los descartes de fraude. La solución permitirá al Jefe de Monitoreo de Alertas, visualizar a través de un cuadro de mandos el desempeño de cada uno de los agentes, que le permitirá controlar eficientemente los recursos que maneja.

#### **4.6 Roles y responsabilidades del equipo del proyecto**

Los recursos que forman parte del presente proyecto están, básicamente, centrados en el desarrollo técnico de la solución basada en inteligencia artificial, por lo que se limitan a ello.

Bajo esta premisa se ha establecido un enfoque conservador al momento de establecer los recursos que serán necesarios para el logro del proyecto y su puesta en marcha.

La solución representa un producto novedoso ya que está desarrollada en función a los requerimientos del cliente, permitiendo que el sistema se adapte a las necesidades del cliente y no al contrario. La solución se apoya en nuevas tecnologías, en el uso del aprendizaje automático, aprovechando los servicios cloud para el almacenamiento y procesamiento de los datos, lo que permite alta seguridad, disponibilidad e integridad de los datos.

### **Científico de datos**

Personal que estará a cargo del análisis y preparación de los datos, así como la generación de modelos predictivos y analíticos.

### **Experto en soluciones Cloud**

Personal que se encargará de evaluar aspectos técnicos relacionados a uso de servicios Cloud, migraciones a entornos cloud, conexiones, configuraciones, integración y desarrollo de interfaces para el despliegue de la solución en un entorno cloud.

### **Analista Programador**

Rol que estará a cargo de la codificación del sistema, desarrollo de interfaces de usuario y la construcción del código fuente de toda la lógica del negocio para el desarrollo de la solución.

### **Analista de Base de datos**

Personal, que se dedicará a realizar un análisis exploratorio de los datos a través de consultas, cruce de información, creación y gestión de la base de datos.

## **Agile coach**

Personal, que estará a cargo de la supervisión del cumplimiento de las metodologías ágiles, para la obtención temprana del producto mínimo viable y sobre ello obtener el producto en función a las necesidades del cliente.

### **4.7 Cronograma y riesgos iniciales del proyecto**

El presente proyecto tendrá una duración aproximadamente de cuatro meses, mediante el uso de metodologías ágiles basado en entregables para la obtención del producto final.

El presente proyecto se materializa en una solución de detección de fraudes, que busca generar un producto que cumpla con los requerimientos presentados por el banco peruano. Para el desarrollo y planificación del proyecto se formará a equipos especialistas, que trabajarán de manera sinérgica, para la elaboración del producto.

Con el objeto de conocer los requerimientos funcionales y no funcionales que deberá tener la solución, es importante que un representante del banco pueda manifestar e indicar claramente a nivel de detalle las características que deba tener la solución.

Previo al desarrollo de la solución, se llevará a cabo una reunión, donde el personal del banco y el Agile Coach, desarrollaran abiertamente los puntos que se muestran a continuación:

- Aspectos generales de la solución, quiénes son los usuarios que usarán el sistema en el día a día y detalles de las necesidades a cubrir.
- La arquitectura a alto nivel de la solución y los elementos que forman parte de ella para adaptar el sistema dentro de la arquitectura del cliente.
- Definición del tiempo que tomará desarrollar el producto y dimensionar los recursos necesarios tanto físicos como recursos de software.
- Construcción de Product Backlog para la obtención del producto final requerido por el cliente.

A lo largo de los cuatro meses que dura el proyecto se realizarán 4 sprints con una duración de 30 días con sus respectivas revisiones al final de cada sprint, a fin de que el equipo a cargo del desarrollo muestre el detalle de lo avanzado y mostrar los inconvenientes que se obtuvieron para lograr los objetivos de cada sprint en caso existiese. Por otro lado, al final de cada Sprint Review se llevará a cabo un nuevo Sprint Planning, en donde se definen y establecen las nuevas historias de usuario del próximo Sprint. Cada nuevo avance será validado y discutido de manera sinérgica con los involucrados en el proyecto.

Los riesgos iniciales que se tuvo en una primera instancia es tratar de poder definir la necesidad del negocio y poder delimitar el alcance de la propuesta, así como la planificación de las actividades asignadas a cada uno de los involucrados en el proyecto y el compromiso, por supuesto, del equipo de proyecto con la culminación de los entregables.

Tal como se mencionó anteriormente, se establecerá una reunión previa con los líderes del banco para el levantamiento de la información con el Agile Coach. Posteriormente se llevará a cabo una reunión Kick Off, en la cual se convoca a todos los participantes del proyecto y se asignará tareas en relación con las habilidades y destrezas de cada uno, la reunión servirá básicamente para establecer un Road Map y lista de actividades iniciales que sirven para poner en marcha el proyecto.

En la figura 4.4, se muestra el cronograma de actividades del proyecto desde la fase de inicio respecto a la reunión Kick Off, el desarrollo de las actividades del Product Back Log en los cuatro Sprints de 30 días y finalmente la entrega del producto.

El detalle con la duración de cada una de las actividades y los plazos respectivos se muestran en la siguiente tabla.

**Tabla 4.2***Cronograma de actividades*

<b>Actividad</b>	<b>Días</b>	<b>Inicio</b>	<b>Fin</b>
<b>Reunión Inicial – Kick Off</b>	1	01/06/2020	01/06/2020
Definición de requerimientos funcionales	1	04/06/2020	04/06/2020
Definición de requerimientos no funcionales	1	05/06/2020	05/06/2020
Configuración de Procesos	5	07/06/2020	11/06/2020
<b>Sprint 1</b>	29	08/06/2020	07/07/2020
Reunión con Agile Coach	1	08/07/2020	08/07/2020
Planificación	1	09/07/2020	09/07/2020
<b>Desarrollo del Producto</b>	21		
Diseño de Base de Datos	4	10/07/2020	13/07/2020
Modelamiento de Base de Datos	3	14/07/2020	17/07/2020
Desarrollo de la Arquitectura de solución	13	18/07/2020	30/07/2020
Reunión de Retrospectiva	1	31/07/2020	31/07/2020
<b>Sprint 2</b>	30	01/08/2020	30/08/2020
Reunión con Agile Coach	1	02/08/2020	02/08/2020
Planificación	1	03/08/2020	03/08/2020
<b>Desarrollo del Producto</b>	28		
Desarrollo Back-end	13	04/08/2020	16/08/2020
Desarrollo Front-end	14	17/08/2020	30/08/2020
Reunión Retrospectiva	1	31/08/2020	31/08/2020
<b>Sprint 3</b>	30	01/09/2020	30/09/2020
Reunión con Agile Coach	1	02/09/2020	02/09/2020
Planificación	1	03/09/2020	03/09/2020
<b>Desarrollo del Producto</b>			
Desarrollo de algoritmo de aprendizaje automático	14	04/09/2020	17/09/2020
Desarrollo de interfaz gráfica web	13	18/09/2020	30/09/2020
Reunión retrospectiva	1	01/10/2020	01/10/2020
<b>Sprint 4</b>	30		
Reunión con Agile Coach	1	02/10/2020	02/10/2020
Planificación	1	03/10/2020	03/10/2020
<b>Pruebas del Producto</b>			
Desarrollo de pruebas unitarias	12	04/10/2020	15/10/2020
Validación de pruebas	13	16/10/2020	28/10/2020
Reunión retrospectiva	1	29/10/2020	29/10/2020
Entrega del Producto	1	30/10/2020	30/10/2020

Para la determinación de los requerimientos y funcionalidades de las características que debe presentar el sistema, se ha determinado las siguientes historias de usuario.



**Tabla 4.3**

*Historia de Usuario - Ingreso al sistema como usuario administrador*

<b>HU1: Ingreso al sistema como usuario administrador</b>	
<b>Como</b>	Administrador
<b>Quiero</b>	Ingresar al sistema con un identificador de usuario y una contraseña
<b>Para</b>	Tener acceso al visor de alertars de fraude, visor de reportes estadísticos.

**Tabla 4.4**

*Historia de Usuario - Gestión de usuarios al sistema*

<b>HU2: Gestión de usuarios al sistema</b>	
<b>Como</b>	Administrador
<b>Quiero</b>	Acción de crear y eliminar los usuarios para el acceso al sistema
<b>Para</b>	Utilizar el sistema en función al perfil del usuario

**Tabla 4.5**

*Historia de Usuario - Gestión de cambio de contraseña*

<b>HU3: Gestión de cambio de contraseña</b>	
<b>Como</b>	Usuario administrador, usuario analista, usuario agente monitoreo
<b>Quiero</b>	Realizar el cambio de la contraseña asignada.
<b>Para</b>	Garantizar la seguridad de mi usuario y las tareas relacionadas.

**Tabla 4.6***Historia de Usuario - Exportar data en archivo excel*

<b>HU4: Exportar data en archivo excel</b>	
<b>Como</b>	Usuario administrador, usuario analista, usuario agente monitoreo.
<b>Quiero</b>	Exportar las operaciones fraudulentas alertadas para gestiones relacionadas a través de un icono en el visor de alertas de fraude.
<b>Para</b>	Tener una bitácora de transacciones gestionadas por el agente de monitoreo.

**Tabla 4.7***Historia de Usuario - Notificar alertas que llegan al sistema*

<b>HU5: Notificar las alertas que llegan al sistema</b>	
<b>Como</b>	Usuario agente monitoreo
<b>Quiero</b>	Se notifique a través de un mensaje de diálogo, en el sistema web, todas las alertas que llegan al visor de fraude.
<b>Para</b>	Refrescar la página en caso no se muestren las nuevas alertas en el visor de fraude.

**Tabla 4.8***Historia de Usuario - Marcaje manual de fraude en visor*

<b>HU6: Marcaje manual de fraude en visor</b>	
<b>Como</b>	Administrador, Usuario agente monitoreo
<b>Quiero</b>	Marcar las transacciones alertadas en el visor de fraude, en caso se confirme el fraude, se debe marcar a través de un checkbox.
<b>Para</b>	Para tener etiquetados los casos confirmados de fraude.

**Tabla 4.9**

Historia de Usuario - Generación de Informe de indicadores de fraude

<b>HU7: Generación de informe de indicadores de fraude</b>	
<b>Como</b>	Administrador, analista de fraude
<b>Quiero</b>	Descargar el contenido de los reportes y dashboard en formato pptx y pdf.
<b>Para</b>	Para la presentación de los gráficos en los comité semanales del área para mostrar los indicadores.

**Tabla 4.10**

Historia de Usuario - Ingresar comentario como referencia a las transacciones gestionadas

<b>HU8: Ingresar comentario de referencias de las transacciones gestionadas</b>	
<b>Como</b>	Agente de Monitoreo.
<b>Quiero</b>	Ingresar una descripción de las transacciones que son atendidas por el agente de monitoreo.
<b>Para</b>	Tener una referencia del cliente ante un nuevo posible caso de fraude.

Luego de haber identificado las historias de usuarios, con sus respectivas especificaciones y descripciones, estas serán implementadas en los sprint; sin embargo, es necesario definir el Product Backlog, que constituye las actividades realizadas por cada Sprint.

**Tabla 4.11***Product Backlog*

<b>Sprint</b>	<b>HU</b>	<b>Descripción</b>	<b>Tareas</b>
<b>Primer Sprint</b>	HU1	Ingreso al sistema como usuario administrador	<b>T1:</b> Elaborar el diseño de la base de datos y creación de relaciones entre tablas <b>T2:</b> Diseñar el esquema de base de datos. <b>T3:</b> Desarrollar la interfaz gráfica del login de acceso al sistema. <b>T4:</b> Creación de usuario administrador a nivel de base de datos.
	HU2	Gestión de usuarios al sistema	<b>T5:</b> Desarrollar el código para creación de usuarios a partir del usuario administrador.
	HU3	Gestión de cambio de contraseña	<b>T6:</b> Implementar la lógica de cambio de contraseña en el código.
<b>Segundo Sprint</b>	HU4	Exportar data en archivo excel	<b>T5:</b> Desarrollar una funcionalidad de exportar data.
	HU5	Notificar las alertas que llegan al sistema	<b>T6:</b> Desarrollar un objeto en el código con los parámetros de notificación.

(continúa)

(continuación)

<b>Sprint</b>	<b>HU</b>	<b>Descripción</b>	<b>Tareas</b>
<b>Tercer Sprint</b>	HU6	Marcaje manual de fraude en visor	<b>T7:</b> Implementar la funcionalidad a través de un checkbox.
<b>Cuarto Sprint</b>	HU7	Generación de informe de indicadores de fraude	<b>T8:</b> Desarrollar la funcionalidad para exportar el contenido de los indicadores en formato pdf.
	HU8	Ingresar comentario de referencias de las transacciones gestionadas	<b>T9:</b> Funcionalidad que permite, a través de un text box, ingresar contenido de texto.

#### **4.8 Medidas de control (indicadores)**

Uno de los indicadores de medición del proyecto, es la identificación del falso positivo, que permite identificar que tan efectiva es la solución que permitirá identificar el fraude

$$\text{Falso positivo} = \frac{\text{Número de transacciones fraudulentas}}{\text{Total de transacciones genuinas}}$$

Mediante dicho indicador, se podrá medir la efectividad del sistema para detectar el fraude en tiempo real.

#### **4.9 Recursos y presupuesto**

En el apartado 4.6 de Roles y responsabilidades del equipo de proyecto ya se definió las tareas de cada uno de los miembros responsables a cargo del proyecto por lo que en esta sección se detallará el presupuesto asignado a cada uno de los recursos involucrados.

### **Científico de datos**

El perfil del profesional científico de datos se orienta al análisis de la información y desarrollo de modelos predictivos para generar cambios y mejoras durante el desarrollo de la solución.

Los costos por los servicios del profesional científico de datos son de S/. 8,000 mensuales.

### **Analista Programador**

El profesional analista programador se encargará de la codificación necesaria para la elaboración de la solución, mantenimiento, actualización de la base de datos. Además de realizar pruebas y cambios constantes de la lógica de negocio para el diseño de los algoritmos de Machine Learning. Los costos incurridos por los servicios del profesional son de S/. 5,500 mensuales.

### **Analista Base de Datos**

El profesional analista de base de datos se dedicará a construir el modelo de base de datos y la relaciones que existirán entre las diferentes tablas para la estructura lógica de la solución a nivel de base de datos. A su vez se encargará del mantenimiento de esta.

El presupuesto asignado para dicho personal es de S/12,000 por los cuatro meses que dure la implementación del proyecto.

### **Experto en soluciones Cloud**

Profesional cuya principal función estará a cargo de evaluar los diferentes servicios que ofrecen las plataformas basadas en la nube (Amazon Web Services, Microsoft Azure, Google Cloud Platform), a fin de determinar cuál es la que mejor se adapta a la arquitectura diseñada para la solución en Confluent Cloud. Además, estará a cargo de la puesta en producción de la solución basada en Machine Learning. El presupuesto asignado para dicho personal es de S/18,000 durante los cuatro meses que tome el desarrollo de la solución.

## **Agile Coach**

Profesional, que velará el cumplimiento, a cabalidad, del marco de referencia Scrum y fomentará el trabajo en equipo, ayudará a la resolución de problemas que se pueda presentar en el transcurso del proyecto y bajo un enfoque de escucha activa, tratará de entender cada aspecto que motive o desanime del personal y promover la empatía, a fin de hacer que la productividad sea mayor y la sensación sea satisfactoria. Se encargará de orquestar de la mejor manera posible al equipo de trabajo a fin de que cada uno de los miembros desempeñe sus tareas de manera eficiente y eficaz. La responsabilidad del Agile Coach es indispensable ya que tiene un enfoque más general y promueve la armonía dentro del equipo mediante técnicas del manifiesto ágil que ayudan a cada uno de los miembros del equipo a lograr sus objetivos y por consiguiente al desarrollo integral del proyecto. El presupuesto asignado para el especialista es de S/ 16,000.

Por otro lado, con respecto a los recursos de hardware que se utilizarán para la construcción de la solución, este no tiene costo alguno dado que cada involucrado en el desarrollo del proyecto posee un equipo de hardware (pcs o laptops) para la realización de sus respectivas tareas. Lo correspondiente a recursos de software, se utilizarán herramientas open source tales como IntelliJ IDEA como IDE para el desarrollo de la solución (elaboración del código fuente), Dbeaver, un gestor para la administración de la base de datos. Con respecto al despliegue de la solución se necesitará hacer uso de los servicios basados en la nube de Confluent Cloud, que involucra el mantenimiento de los datos y el procesamiento para la generación de alertas de fraude. El costo mensual por estos servicios es de S/ 707.72.

## **CAPÍTULO V: DESARROLLO DEL PROYECTO**

La construcción del Producto Mínimo Viable (MVP) del presente proyecto se llevará a cabo bajo la metodología del Design Thinking, la cual está orientada a generar ideas innovadoras implementadas como un prototipo, a partir de la identificación oportuna de la necesidad presentada.

### **5.1 Empatizar**

Uno de los primeros pasos que involucra la metodología del Design Thinking es empatizar; es decir, conocer el sentir del usuario. El usuario sobre el cual estará diseñado la solución es el Analista de Fraudes de un Banco Peruano, y para ello se ha recurrido a entrevistas periódicas a fin de recopilar toda la información posible sobre cuáles son los problemas presentados, qué es lo que lo motiva a apostar por una solución innovadora y qué espera de ella.

#### **5.1.1 Entrevistas**

La entrevista se realizó a través de una video llamada, cuyo principal objetivo fue tratar de conocer cuál es la situación actual, cuáles son los problemas que afronta el analista y las consecuencias de estos y su impacto en el banco. Nos permite hacer un diagnóstico más exhaustivo en base a la experiencia del colaborador del Banco.

En la tabla 5.1 se detallan las preguntas con sus respectivas respuestas dadas por el analista de fraude.



**Tabla 5.1**

## Preguntas de Entrevista

<b>Preguntas</b>	<b>Respuesta</b>
1. ¿Cuáles son sus principales funciones dentro del banco?	Soy responsable de coordinar las divisiones de Monitoreo de Fraudes y Reclamos. Genero reportes e indicadores de gestión para medir el trabajo del personal. Estoy a cargo de la gestión de reglas para prevenir el fraude en todos los canales del banco.
2. ¿Cuál es la principal preocupación a nivel de área dentro del banco?	La principal preocupación se resume, a que los índices de fraudes y de reclamos por consumo no reconocido en el canal de comercio electrónico se ha incrementado y agudizado más aun por la pandemia COVID-19. La gestión dentro del área no está centralizada. Además, no hay personal suficiente para las diferentes tareas que existen como área, siendo el área de prevención de fraudes un área crítica del negocio. Finalmente, las reglas para la detección del fraude que maneja el Banco a través de su sistema es ineficiente lo que implica un alto número de operaciones fraudulentas, lo que implica que se incremente la cantidad de recursos y por ende se genere demoras en la gestión.
3. ¿Cómo gestiona el trabajo dentro del área?	El trabajo, hasta antes de la Pandemia, lo gestionada a través de reuniones semanales todos los lunes, para evaluar el desempeño de cada uno y plantear sugerencias e ideas en beneficio del área; sin embargo, producto de la pandemia, este procedimiento se volvió más complejo para llevarlo dado que todo el personal del área está en modalidad Teletrabajo con tareas preestablecidas, dificultándose.
4. ¿Cómo define la reputación del área de prevención de fraudes?	La reputación del área se ha visto reflejada en ratios negativos, debido a las altas pérdidas monetarias por los fraudes, además de la demora en la atención de los reclamos y una gestión regular de las llamadas a clientes.
5. ¿Cuáles son los principales problemas que afronta usted como analista de fraudes?	Los problemas que presenta el banco radican en la falta de visibilidad de las transacciones a través de un sistema, lo que no permite hacer un análisis y determinar patrones. La ausencia de un motor de fraudes nos dificulta la gestión dentro del área y una carga extra por los procedimientos manuales. Actualmente, estamos teniendo casos de phishing que son detectados, a través de consultas a través de sistemas del banco y llamando directamente al cliente, cuando esto se podría detectar fácilmente con desarrollo de un motor

(continúa)

(continuación)

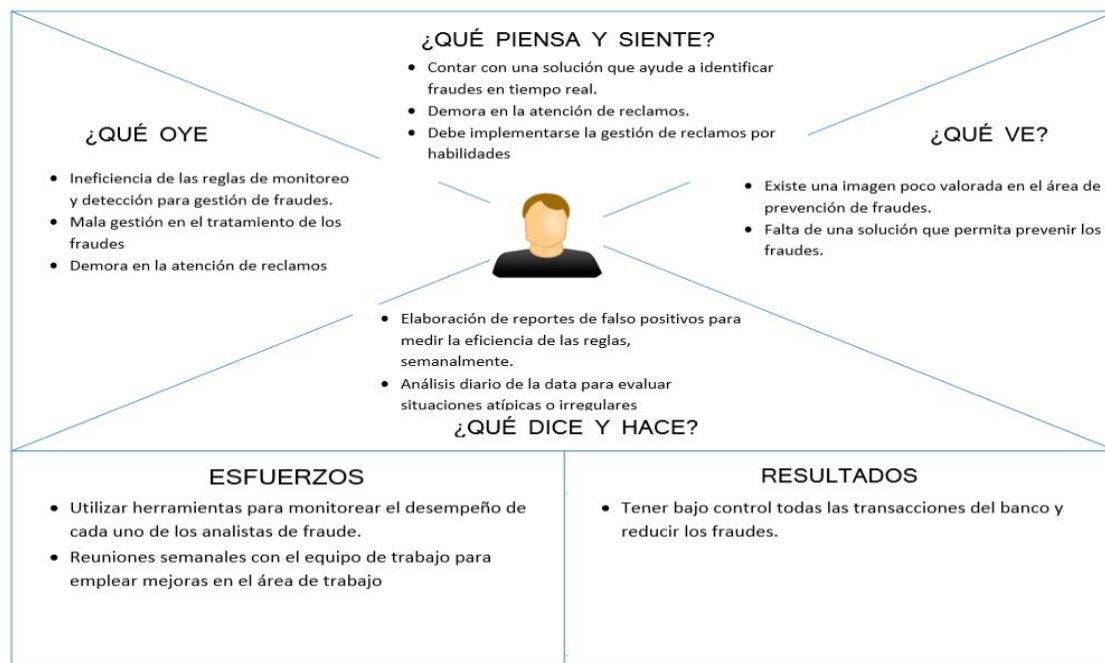
Preguntas	Respuesta
	de fraude. Además la herramienta que nos proporciona Visa, VRM, nos permite crear reglas, pero la información que viaja en la trama de la operación no se tiene el nombre del cliente y datos personales del mismo, porque no se ha hecho una solución integral, las reglas que se manejan en dicha plataforma se hacen en función a montos y cantidades atípicas por tarjeta, puesto que no se tiene información del cliente, como para saber si es un cliente que compra por internet o no tiene patrón de consumos en ese canal para así definir reglas eficientes y prevenir el fraude. Como banco, manejamos otros canales (cajeros automáticos, agentes, banca móvil, etc.) cuya información no viaja por el VRM y también sería una buena oportunidad de mejora integrar todos los canales a través de un motor de fraude; sin embargo, en términos de pérdidas monetarias tenemos mayor impacto por las transacciones hechas por comercio electrónico.
6. ¿Qué acción inmediata debería adoptar el área para una mejor gestión y prevención del fraude?	Adquirir una solución de fraude basada en reglas de monitoreo e inteligencia artificial que optimice la detección del fraude, automatizar los procesos manuales que existen dentro del área a fin de realizar las gestiones de manera eficiente. Incrementar los recursos humanos para las gestiones de monitoreo (llamar al cliente) para hacer descarte de fraudes.

### 5.1.2 Mapa de Empatía

Se empleó el mapa de empatía como una herramienta, para consolidar la etapa “Empatizar” para conocer y entender la realidad del usuario, sus frustraciones y generadoras de alegrías. El proceso de empatía hacia el analista de fraudes es fundamental y comprende el esfuerzo por entender al usuario y la forma de cómo ve la situación actual, cómo hacen las cosas, sus necesidades físicas y emocionales, cómo piensan y qué es lo realmente valioso para ellos. Para la construcción del mapa de empatía, se ha tomado como base mi experiencia cuando me desempeñé como colaborador dentro del Banco en el área de Prevención de Fraudes y sobre la entrevista que se tuvo con el Analista de Fraudes, en lo que refiere que la situación no ha variado y la falta de recursos para el desempeño de actividades dentro del área también ha impactado negativamente en el Banco.

**Figura 5.1**

*Mapa de Empatía*



## 5.2 Definir

Recopilar información del usuario a través de entrevistas y el mapa de empatía, ayudó a conocer con mayor profundidad los problemas, los generadores de alegrías y frustraciones. Con esta información se identificó la necesidad que existe, a través del relevamiento del problema central, que constituye en la ineficiencia del sistema de fraudes del banco, que no permite detectar el fraude consistentemente, lo que origina una gestión ineficiente en la gestión, prevención, detección y tratamiento del fraude. Luego de identificar el problema principal, se identificó y definió la siguiente necesidad:

*La necesidad que busca cubrir el presente proyecto es la de brindar un apoyo al analista de fraudes a través de una solución tecnológica dinámica y escalable que permite detectar y evitar el fraude, el cual constituye en numerosas pérdidas económicas, pérdidas de reputación y la inversión en numerosos recursos para el tratamiento de fraudes.*

Un aspecto importante de esta etapa según la metodología del Design Thinking es definir al usuario que usará el producto innovador a través de una solución tecnológica, la definición del usuario se detalla a continuación:

*El perfil del usuario, para quien se diseñó la solución, es un economista de 35 años, quien tiene una esposa y no tiene hijos, que desempeña el cargo de analista de prevención de fraudes. Al usuario le preocupa la cantidad de reclamos por consumos no reconocidos en el canal internet, las grandes pérdidas monetarias por fraudes y una mala reputación del área de fraudes ocasionada por el alto volumen de reclamos y un sistema basado en reglas ineficientes de fraude, demora en resolución de reclamos y una gestión ineficiente en la recepción de llamadas de clientes, debido a la falta de recursos humanos.*

### **5.3 Idear**

Una vez identificada la necesidad del cliente, se procede con el proceso del diseño y la generación de múltiples ideas para creaciones innovadoras, cabe mencionar que todas las ideas son válidas y que generan aportes de gran valoración para la búsqueda de posibles soluciones.

Se detalla a continuación el concepto de la idea de solución empezando por el problema que se intenta resolver. A partir de ello se busca que, mediante una plataforma, disminuir la cantidad de transacciones fraudulentas y mejorar la reputación del área dentro del banco, así como una gestión integral y eficiente a través de un sistema centralizado que ofrezca un diseño de fácil uso y entendimiento.

#### **5.3.1 Brainstorming**

Se aplicó la técnica de lluvia de ideas entre el analista de fraudes, jefe de Monitoreo y analistas de reclamos, a fin de poder plasmar ideas abiertas acerca de cómo sería su propuesta de solución a nivel técnico y funcional del sistema, así como las características que debe tener esta para el logro de objetivos y mejorar la eficiencia en la detección, prevención y tratamiento del fraude financiero. Cabe mencionar que la gran mayoría de ideas se basan en una plataforma web, cuya disponibilidad sea 24 horas al día y 7 días a la semana (24x7), que ofrezca reportes gráficos de alto nivel y sea efectivo para prevenir el fraude para una mejor gestión a nivel de área interna dentro del banco. Además, algunos

participantes manifestaron su incomodidad y poca satisfacción del sistema actual del banco, que se basa en reglas estáticas y, finalmente, cuál es la percepción del usuario final sobre los problemas que traen la ocurrencia del fraude.

**Figura 5.2**

*Brainstorming*



## 5.4 Prototipar

Luego de aplicar diferentes técnicas, que se explican a lo largo del presente documento, para conocer e identificar las necesidades se procede al “prototipeo” la solución, que consiste en la construcción del producto mínimo viable (MVP) en función a las características ofrecidas por el usuario final.

El componente técnico de la solución está basado en inteligencia artificial mediante la implementación del algoritmo Random Forest, si bien los diseños y las características visuales son importantes, es necesario indicar que el componente vital es la aplicación funcional del algoritmo para detectar fraudes hechos por comercio electrónico.

Los criterios establecidos para el desarrollo de la solución son innovadores para el banco peruano en particular porque implica dejar de lado prácticas antiguas para la gestión de la herramienta de detección de fraude como por ejemplo, demora en el proceso de descarte de un fraude, a causa de la búsqueda de información del cliente en muchos sistemas y por otro lado es que la plataforma ofrecerá una herramienta con gráficos estadísticos que faciliten al analista la toma de decisiones en tiempo real.

El sistema que se implementará se basa en el uso de nuevas tecnologías basadas en machine learning, tecnologías basadas en cloud e implementación del algoritmo Random Forest, la cual se perfila perfectamente para solucionar problemas de clasificación como es el caso de estudio, puesto que se busca determinar, bajo ciertas características, aquellas transacciones fraudulentas y transacciones genuinas de manera dinámica y en tiempo real.

Los beneficios que se obtendrán con la solución permiten una mejor gestión y control de las transacciones hechas por comercio electrónico a través de gráficos dinámicos y reportes de alto nivel, que no solo permiten detectar el fraude a través de un visor, sino que ayuda al analista a tomar decisiones de negocio.

#### **5.4.1 Prototipado de la solución**

En el acápite anterior, se definió la solución que se desea implementar y se ha diseñado pantallas de la solución requerida por el usuario.

Las características que debe tener el sistema son las siguientes:

- Gestión de perfiles a través de usuario y contraseña para el acceso al visor de transacciones fraudulentas por comercio electrónico.
- A través del visor, el analista de monitoreo podrá visualizar las transacciones fraudulentas a nivel de detalle para, luego, ponerse en contacto con el cliente y hacer el descarte de fraude.
- La herramienta de reportes permitirá la visualización del top 10 de los comercios que tienen la mayor cantidad de fraudes en tiempo real. Además, se mostrarán datos del ticket promedio de clientes agrupados por comercio y reportes acumulados de las operaciones realizadas en comercio electrónico en tiempo real. Finalmente, se

mostrará los indicadores de desempeño por cada usuario analista de monitoreo de fraudes.

El código fuente de la solución se encuentra en el apartado de anexos.

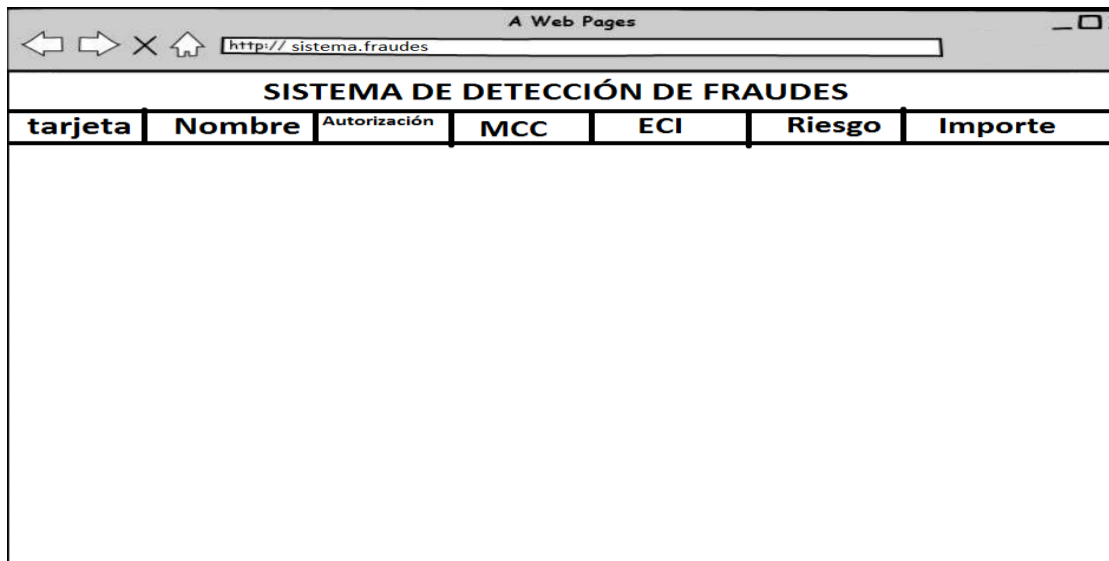
### Figura 5.3

#### Pantalla de Login

The screenshot shows a web browser window titled "A Web Pages" with the address bar containing "http://sistema.fraudes". The page content is displayed on a grid background. At the top, there is a header bar with the text "Bienvenido usuario, crayo" on the left and "SISTEMA DE DETECCIÓN DE FRAUDES" in the center. Below this, a login form is centered. The form has two input fields: "Usuario" with the value "crayo" and "Contraseña" with the value "\*\*\*\*\*". Below the password field is a checkbox labeled "Olvidó contraseña?". At the bottom of the form are two buttons: "Ingresar" and "Cancelar".

**Figura 5.4**

*Visor de transacciones fraudulentas*



**Figura 5.5**

*Visor de Reportes Estadísticos*





## Descripción de la fuente de datos

La data sobre la que se construirá la solución corresponde a transacciones realizadas en Internet con tarjeta de crédito durante los años 2018 y 2019. Esta información se obtuvo del sistema denominado VRM (Visa Risk Manager), solución que maneja el banco, actualmente, para la gestión de alertas y declinaciones basadas en reglas. La data comprende 3,960 transacciones catalogadas como fraudes y 56,047 transacciones consideradas genuinas. Es importante mencionar que, dentro del universo de operaciones etiquetadas como fraudes, se han incluido aquellas transacciones rechazadas por alguna regla que se ha implementado.

A continuación, se definirá las variables más representativas de la fuente de datos.

**Tabla 5.2**

### *Definición de variables*

N°	Nombre de variable	Descripción	Valores
1	Número de Tarjeta	Número de tarjeta del cliente	4313*****5016
2	Edad	Edad del cliente	23,30,50
3	MCC (Merchant Category Code)	Código que identifica la categoría del comercio o establecimiento donde se hizo la operación.	MCC: 5311 Código que identifica a los comercios relacionados a tiendas por departamento. Existen diversos códigos.
4	Calificación de Riesgo	Corresponde al nivel de riesgo que está sujeta la transacción.	82; identifica a la transacción como muy riesgosa. Aquellos valores mayores a 60, se considera como una transacción en riesgo, posible caso de fraude
5	MOTO-ECI	Nivel de seguridad por medio de la cual se hace la transacción	Los valores correspondientes al campo ECI son los siguientes: 05, para transacciones realizadas por comercio electrónico en un ambiente seguro.

(continúa)

(continuación)

N°	Nombre de variable	Descripción	Valores
			06, cuando las transacciones no son autenticadas o no son seguras, porque el comercio no tiene la tecnología de 3-D Secure.
			07, corresponde a transacciones sin autenticar y consideradas poco seguras.
6	Expiration Date Digit	Variable que indica si durante la transacción se hizo el ingreso de la fecha de expiración de la tarjeta	0; cuando no involucra el ingreso de la fecha de expiración de la tarjeta. 1; cuando se digita la fecha de expiración de la tarjeta.
7	Modo de Entrada	Variable que indica el medio por la cual se captaron los datos de la tarjeta, durante la compra.	01; indica que se hizo la operación con tarjeta no presente; es decir, sin la intervención del POS. 10; indica que la operación se hizo con tarjeta no presente, sin embargo, al ser una operación recurrente, los datos de la tarjeta han sido ya previamente guardados en las bases de datos del comerciante.
8	Código de moneda	Variable que especifica el tipo de moneda que se procesa durante la transacción	Código 840; indica que la transacción se procesó en moneda extranjera(dólares) Código 604; indica que la transacción se procesó en moneda local (soles).
9	Código de Autorización	Variable que describe el número generado producto de una transacción exitosa	Los valores que puedan tomar esta variable son diversos. Se presentan algunos ejemplos a continuación:

(continúa)

(continuación)

N°	Nombre de variable	Descripción	Valores
			371638
			555375
10	Código de respuesta	Variable relacionada a la descripción y estado de la transacción.	51; rechazado por saldo insuficiente. 00; transacción exitosa 05; rechazado por el banco emisor de tarjeta. Código 59; rechazado por regla.
11	Importe	Variable que describe el monto (en soles) por la cual se procesó la transacción	S/.120 S/150 S/.50

## Exploración de la data

Figura 5.6

Visualización de datos

TARJETA	NOMBRE	APELLIDO	CODIGO_TRX	FECHA_TRX	HORA_TRX	ECI	categoria MCC	Descripcion	Importe
4214100187749550	PONTE	TERRY	982008	2019-02-01T00:00:00.000+05:21083	10:25:44	7	TIENDAS POR DEPARTAMENTOS	WISH.COM	210.19
4214100200235160	LAMA	JARA	902374	2019-02-01T00:00:00.000+05:21084	10:50:51	7	TIENDAS POR DEPARTAMENTOS	WISH.COM	238.82
4214100202120400	URBINA	PLAZA	323053	2019-02-01T00:00:00.000+05:21085	15:27:13	7	Digital Goods ♦ Applications (Excludes Games)	GOOGLE *Youdagames	87.99
4214100172057380	MESTANZA	MESTANZA	185445	2019-02-01T00:00:00.000+05:21086	15:27:13	7	Digital Goods ♦ Applications (Excludes Games)	GOOGLE *Youdagames	87.99
4214100181543680	BARRETO	CERNA	723064	2019-02-01T00:00:00.000+05:21087	15:05:38	7	INSTITUCIONES FINANCIERAS ♦ MERCANCIA Y SERVICIOS	YAPE	150
4214100191533810	LOPEZ	MENDOZA	604452	2019-02-01T00:00:00.000+05:21088	03:08:51	7	REDES DE COMPUTADORAS / SERVICIOS DE INFORMACION	ruffyvpn.net	381.47
4214100186815170	VILLARREAL	SANCHEZ	233024	2019-02-01T00:00:00.000+05:21089	16:30:53	7	INSTITUCIONES FINANCIERAS ♦ MERCANCIA Y SERVICIOS	BANCO RIPLEY	462.3
4214100171589890	SANJINEZ	PASCO	442096	2019-02-01T00:00:00.000+05:21090	11:36:56	7	Direct Marketing – Inbound Telemarketing Merchants	MEE*STAFFSETT.COM	105.18
4214100161430730	ALTAMIRANO	ORBEZO	580339	2019-02-01T00:00:00.000+05:21091	17:47:27	7	ESTABLECIMIENTOS DE JUEGOS DE VIDEO Y MQUINAS DE RECREACION	STEAMGAMES.COM	75
4214100160067620	SALVADOR	PILCO	474232	2019-02-01T00:00:00.000+05:21092	15:46:11	7	VENTAS DE SEGUROS, GARANTIAS Y PRIMAS	CE RIMAC SEGURO	60
4214100197980870	CUADRADO	CIPRIANO	734067	2019-02-01T00:00:00.000+05:21093	10:16:25	7	TIENDAS POR DEPARTAMENTOS	WISH.COM	337.15
4214100199239920	CUADROS	ALVA	536473	2019-02-01T00:00:00.000+05:21094	14:33:47	7	SERVICIOS DE TELECOMUNICACION INCLUYENDO LLAMADAS LOCALES Y DE LAR...	CLARO APP MI CLARO	163.87
4214100160285770	TELLO	SILVA	830363	2019-02-01T00:00:00.000+05:21095	15:25:59	7	SERVICIOS ELECTRICIDAD, AGUA, SANITARIOS	CE LUZ DEL SUR	383.7
4214100194587770	ROJAS	HERRERA	595487	2019-02-01T00:00:00.000+05:21096	20:44:13	7	SERVICIOS ELECTRICIDAD, AGUA, SANITARIOS	CE LUZ DEL SUR	383.7
4214100196843750	OSORIO	NAPURI	290064	2019-02-01T00:00:00.000+05:21097	03:04:55	7	Large Digital Goods Merchant	HUGEGAME.NET	61.46
4214100153035820	OUICA ♦	JU ♦	847450	2019-02-01T00:00:00.000+05:21098	20:11:17	7	Large Digital Goods Merchant	sanchna.net	61.46
4214100185767200	DEL	PECHE	177986	2019-02-01T00:00:00.000+05:21099	10:51:17	7	INSTITUCIONES FINANCIERAS ♦ MERCANCIA Y SERVICIOS	BANCO RIPLEY	162.75
4214100203918810	VILLEGAS	AMARANTO	293924	2019-02-01T00:00:00.000+05:21100	10:50:38	7	TIENDAS POR DEPARTAMENTOS	WISH.COM	129.94
4214100208065920	PAREDES	MEJIA	912671	2019-02-01T00:00:00.000+05:21101	22:11:52	7	INSTITUCIONES FINANCIERAS ♦ MERCANCIA Y SERVICIOS	BANCO RIPLEY	53.75
4214100195749380	ALLAGA	ZAMORA	486880	2019-02-01T00:00:00.000+05:21102	03:28:48	7	TIENDAS DE DESCUENTOS	ALIEXPRESS.COM	71.93
4214100208171750	DE	CORONADO	579324	2019-02-01T00:00:00.000+05:21103	21:39:37	7	TIENDAS DE DISCOS	APPLE.COM/BILL	269.9
4214100210067990	SOTO	SALVADOR	75080	2019-02-01T00:00:00.000+05:21104	14:14:52	7	SERVICIOS ELECTRICIDAD, AGUA, SANITARIOS	SEDAPAL	552.2

Las variables que se han determinado para la implementación y entrenar el modelo son Categoría MCC, Descripción MCC, que corresponden a variables tipo cadena, y la variable Importe que es de tipo numérico.

Para los valores de cadena como los son Descripción y Categoría MCC, se ha utilizado la función de IndiceString que permite transformar los valores a datos numéricos, ya que el algoritmo de Machine Learning Random Forest, no procesa información de tipo cadena.

Los datos de entrada son los campos “Descripción” y “Categoría MCC”, la salida producto de la función IndiceString, tendrá datos numéricos, esas dos columnas son Category Indexed y Merchant\_Indexed, como se observa en la figura 5.7.

**Figura 5.7**

*Transformación de Datos*

cc_num	category	merchant	distance	amt	age	is_fraud	category_indexed	merchant_indexed
5157595343543285	gas_transport	Schmitt Inc	0.73	111.0	46	0.0	0.0	28.0
5157595343543285	kids_pets	Beer-Jast	1.73	66.0	46	0.0	4.0	291.0
5157595343543285	grocery_pos	Hudson-Ratke	1.23	220.0	46	0.0	1.0	310.0
5157595343543285	entertainment	Kassulke Inc	2.17	100.0	46	0.0	9.0	470.0
5157595343543285	shopping_net	Boyer PLC	1.33	80.0	46	0.0	5.0	78.0
5157595343543285	entertainment	Spencer PLC	1.29	141.0	46	0.0	9.0	304.0
5157595343543285	entertainment	Brown-Greenholt	0.8	221.0	46	0.0	9.0	527.0
5157595343543285	travel	Kovacek Ltd	1.5	91.0	46	0.0	13.0	663.0
5157595343543285	gas_transport	Kutch LLC	0.71	57.0	46	0.0	0.0	2.0
5157595343543285	kids_pets	Lowe, Dietrich and Erdman	1.41	158.0	46	0.0	4.0	230.0
5157595343543285	kids_pets	Bednar PLC	1.99	211.0	46	0.0	4.0	101.0
5157595343543285	kids_pets	Hammes-Beatty	0.88	42.0	46	0.0	4.0	242.0
5157595343543285	kids_pets	Hilpert-Conroy	0.97	103.0	46	0.0	4.0	223.0
5157595343543285	gas_transport	Robel, Cummerata and Prosacco	1.26	100.0	46	0.0	0.0	32.0
5157595343543285	grocery_pos	Strosin-Cruickshank	1.02	75.0	46	0.0	1.0	181.0
5157595343543285	grocery_pos	Schultz, Simonis and Little	1.8	65.0	46	0.0	1.0	133.0
5157595343543285	home	Beier and Sons	1.66	112.0	46	0.0	3.0	81.0
5157595343543285	misc_pos	Turner, Ruecker and Parisian	1.81	27.0	46	0.0	7.0	229.0
5157595343543285	entertainment	Howe PLC	1.56	151.0	46	0.0	9.0	201.0
5157595343543285	entertainment	Bauch-Blanda	1.88	126.0	46	0.0	9.0	509.0

only showing top 20 rows

Antes de aplicar la técnica de aprendizaje automático se debe normalizar la data correspondiente a la edad y monto a fin de que estén en una misma escala. Luego dichos valores normalizados se almacenarán en un vector llamado “Rawfeature”.

**Figura 5.8**

*Normalización de los datos*

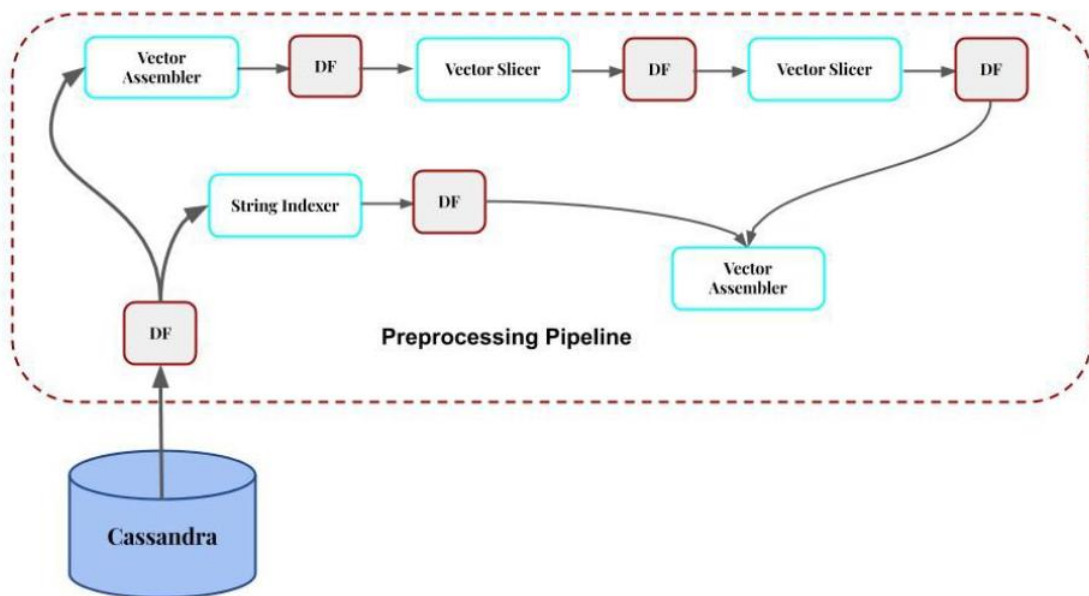
distance	amt	age	is_fraud	category_indexed	merchant_indexed	rawfeature
0.73	111.0	46	0.0	0.0	28.0	[0.73,111.0,46.0]
1.73	66.0	46	0.0	4.0	291.0	[1.73,66.0,46.0]
1.23	220.0	46	0.0	1.0	310.0	[1.23,220.0,46.0]
2.17	100.0	46	0.0	9.0	470.0	[2.17,100.0,46.0]
1.33	80.0	46	0.0	5.0	78.0	[1.33,80.0,46.0]
1.29	141.0	46	0.0	9.0	304.0	[1.29,141.0,46.0]
0.8	221.0	46	0.0	9.0	527.0	[0.8,221.0,46.0]
1.5	91.0	46	0.0	13.0	663.0	[1.5,91.0,46.0]
0.71	57.0	46	0.0	0.0	2.0	[0.71,57.0,46.0]
1.41	158.0	46	0.0	4.0	230.0	[1.41,158.0,46.0]
1.99	211.0	46	0.0	4.0	101.0	[1.99,211.0,46.0]
0.88	42.0	46	0.0	4.0	242.0	[0.88,42.0,46.0]
0.97	103.0	46	0.0	4.0	223.0	[0.97,103.0,46.0]
1.26	100.0	46	0.0	0.0	32.0	[1.26,100.0,46.0]
1.02	75.0	46	0.0	1.0	181.0	[1.02,75.0,46.0]
1.8	65.0	46	0.0	1.0	133.0	[1.8,65.0,46.0]
1.66	112.0	46	0.0	3.0	81.0	[1.66,112.0,46.0]
1.81	27.0	46	0.0	7.0	229.0	[1.81,27.0,46.0]
1.56	151.0	46	0.0	9.0	201.0	[1.56,151.0,46.0]
1.88	126.0	46	0.0	9.0	509.0	[1.88,126.0,46.0]

### Modelo Pipeline de Procesamiento

Spark Pipeline es una secuencia específica de etapas y cada etapa corresponde a un Transformador o un Estimador, estas etapas se ejecutan en orden y de manera secuencial, haciendo que la fuente de datos se transforme a medida que pasa por cada una de las etapas

**Figura 5.9**

*Modelo Pipeline*



*Nota. Representación gráfica de componentes de Stage Pipeline. Adaptado de Real Time Credit Card Fraud Detection is implemented using Spark Kafka, por Narayana, 2018)*

Luego del proceso de la data a través del modelo Pipeline, se procederá a separar la data en data de entrenamiento y data para la prueba, se ha establecido que el entrenamiento corresponderá al 80% de la data y el 20% restante servirá como data de prueba del algoritmo.

Luego de ejecutar el modelo se obtuvo la matriz de confusión para medir la eficiencia de predicción.

**Tabla 5.3**

*Resultados Matriz de Confusión*

Matriz de confusión	Positivo	Negativo
Positivo	2104	2270
Negativo	0	7605

Precisión: 0.4810, la tasa de precisión indica que de todas las transacciones fraudulentas que se ha predicho correctamente, cuáles fueron casos reales de fraude.

De las 2,104 transacciones de fraude, el modelo ha predicho correctamente las 2104 transacciones de fraude como fraude.

De 9,875 transacciones genuinas, el modelo predijo erróneamente 2,270 transacciones como fraude y predijo de manera correcta 7,605 transacciones como operaciones genuinas.

El indicador de falso positivo son las transacciones marcadas como fraudulentas cuando en realidad corresponden a transacciones legítimas. Para el cálculo del indicador se divide el total de operaciones por cantidad de fraudes marcado erróneamente

Total, de Operaciones = 9,875

Fraudes Erróneos = 2,270

Fórmula :  $\frac{9,875}{2,270}$

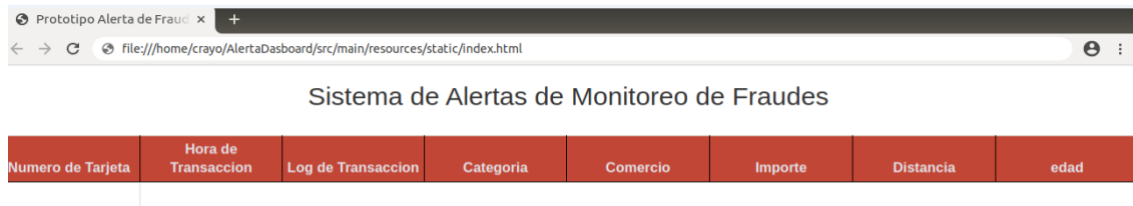
Ratio Falso Positivo: 4.35

Implica que, sobre un total de 10 transacciones marcadas como fraude, 4 corresponden a transacciones genuinas.

Este indicador nos permite medir la eficiencia del algoritmo Random Forest empleado en el prototipo de detección de fraudes ya que nos identifica la tasa de error.

## Figura 5.10

### Interfaz de MVP



Prototipo Alerta de Fraud x +

file:///home/crayo/AlertaDashboard/src/main/resources/static/index.html

Sistema de Alertas de Monitoreo de Fraudes

Numero de Tarjeta	Hora de Transaccion	Log de Transaccion	Categoria	Comercio	Importe	Distancia	edad

## 5.5 Testear

La última etapa dentro de la metodología del Design Thinking es probar la solución con los usuarios interesados.

El usuario probó la solución del módulo del visor de transacciones fraudulentas, para verificar el correcto funcionamiento, si bien es cierto la retroalimentación que se recibió fue buena, aún existen algunos aspectos por mejorar. Por ejemplo, el despliegue de las transacciones se visualiza en tiempo real; sin embargo, cuando se actualiza el navegador del usuario, pierde la visibilidad de las transacciones que se mostraron anteriormente, lo que no permite mapear la cantidad de transacciones revisadas por el analista de monitoreo.

El resultado final del producto mínimo viable si logra satisfacer las necesidades del analista como una versión inicial, puesto que se comprueba la funcionalidad principal que tiene la solución que consiste en mostrar las transacciones fraudulentas en el visor web para la gestión correspondiente. Aunque aún hay algunos aspectos por mejorar la retroalimentación brindada por el usuario durante la prueba fue aceptable en términos de operatividad y funcionalidad.



## CONCLUSIONES

- El campo de la inteligencia artificial es amplio y lo correspondiente al uso de machine learning para la detección de fraudes en internet es una de las tantas aplicaciones que existen, con el desarrollo de nuevas tecnologías y técnicas eficientes relacionadas al Big Data, se podrá diseñar y construir herramientas más robustas y con un alto índice de precisión.
- Si bien es cierto, que para fines del desarrollo del producto mínimo viable se ha implementado el algoritmo Random Forest, en el mundo del Machine Learning, existen diversos algoritmos que se pueden implementar y que se adaptan mejor a determinadas casuísticas o casos de negocio.
- La aplicación del Design Thinking, permitió conocer e identificar los “*insights*” así como abstraer e inducir necesidades, preocupaciones y el sentir del usuario que hará uso de la solución implementada.
- La solución fue diseñada y construida para detectar el fraude por comercio electrónico; sin embargo, uno de los planes es integrar el sistema implementado a los diferentes canales del banco (POS, Retiro, Depósito, entre otros), de tal manera que permita lograr una tasa de mayor efectividad, puesto que se tendría un mayor volumen de información para procesar y que sirva como entrada para el modelo propuesto.
- Un aspecto pendiente del presente proyecto fue la migración del sistema a un ambiente cloud, esto ayudará a que la información y data se encuentren disponibles en cualquier momento y pueda ser consultada. Además, con ello se garantiza la integridad, confidencialidad y disponibilidad de los datos.
- La técnica de minería de datos que se utilizó para la transformación de la data fue la normalización; sin embargo, existen muchas otras técnicas que permiten además buscar patrones y pueden emplearse para predecir el comportamiento futuro en la detección del fraude, gestión del riesgo y resolver los problemas para el tratamiento de grandes volúmenes de datos.

## RECOMENDACIONES

La aplicación de la metodología del Design Thinking ha permitido abstraer un enfoque diferente e innovador en cada una de las etapas de esta metodología, al permitir la supresión de esa idea errónea de pensar primero en el desarrollo del producto sea tangible o intangible, puesto que gracias a la aplicación del mismo, ha permitido llegar a la solución a través de diversas técnicas para evaluar, capturar información y conocer aún más al cliente antes de proponer un diseño basado en el producto en primera instancia.

Para la elaboración del prototipo basado en Inteligencia Artificial se implementó el algoritmo Random Forest que pertenece a la clasificación de Tipo de Algoritmos Supervisados; sin embargo, existen diversos algoritmos bajo esta clasificación que son capaces de resolver problemas relacionados a la detección del fraude.

Actualmente, con el despliegue de las nuevas tecnologías basadas en la nube, es menos complejo contar con un sistema basado en machine learning, puesto que los proveedores de servicios en la nube como Amazon, Microsoft, Google, entre otros. Ya cuentan con soluciones basadas en Inteligencia Artificial, lo que significa que es menos tediosa y más económica, puesto que se ahorra costos en infraestructura física, la adaptación de la solución al caso de negocio en particular.

La implementación de la solución se hizo para el canal de comercio electrónico; sin embargo, para un control total de todas las operaciones de los diversos canales del Banco, se puede integrar la solución con diversos canales como POS, retiros en cajeros automáticos entre otros. A fin de tener un diagnóstico eficiente del fraude e identificar los patrones de consumo por parte del cliente a través de todos los canales.

# GLOSARIO

## **Inteligencia artificial**

La Inteligencia Artificial es la disciplina que investiga la comprensión e imitación de la inteligencia humana, su tarea principal es construir la teoría del procesamiento inteligente de la información con la inteligencia humana realizada por máquinas inteligentes. (Xian, 2010).

## **Machine Learning**

Aprendizaje Automático es un tipo de inteligencia artificial en las que las computadoras están capacitadas para identificar diseños, dentro de grandes volúmenes de datos para mejorar esos ejemplos de forma natural sin la interceptación del ser humano. (Adepoju et al., 2019, p. 2).

## **Design Thinking**

Es una metodología para la innovación diseñada para resolver problemas complejos y encontrar soluciones deseables tomando énfasis en la imaginación, lógica, y el razonamiento sistemático para crear ingeniosos resultados en beneficio de los usuarios. (Anand et al., 2015, p. 69).

## **Minería de datos**

La minería de datos es el proceso de identificar tendencias y patrones valiosos a partir de grandes volúmenes de datos, combinando diferentes campos de estudio como el aprendizaje automático y estadística, requiriendo la capacidad de analizar y manipular datos. (Adepoju et al., 2019, p. 2).

## **Random Forest**

Los bosques aleatorios son conjuntos de árboles de decisión aleatorios, que representan uno de los modelos de aprendizaje automático más exitosos para la clasificación y regresión que combinan muchos árboles de decisión para reducir el riesgo de sobreajuste. (Armel & Dounia Zaidouni, 2019).

## **Fraude**

Es el acto intencional o deliberado de privar a otros, de bienes o dinero por astucia, engaño u otros actos injustos (Sadgal et al., 2019, p. 46).



## REFERENCIAS

- Adepoju, O., Wosowei, J., Lawte, S., & Hemaint, J. (2019). Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques. *2019 Global Conference for Advancement in Technology (GCAT)*, 2.
- Anand, A., Mishra, S., Deep, A., & Alse, K. (2015). Generation of Educational Technology Research. *2015 IEEE Seventh International Conference on Technology for Education*, 69-72.
- ARMEL, A., & Dounia ZAIDOUNI. (2019). Fraud Detection Using Apache Spark. *2019 5th International Conference on Optimization and Applications (ICOA)*, 4.
- Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. *International Conference on Smart Sustainable Intelligent Computing and Applications under ICITETM2020*, 104.
- Crashcourse. (11 de octubre de 2017). Cybersecurity: Crash Course Computer Science #31.[Video] Youtube. Obtenido de [https://www.youtube.com/watch?v=bPVaOIJ6ln0&feature=emb\\_title](https://www.youtube.com/watch?v=bPVaOIJ6ln0&feature=emb_title)
- Hussain Mahdi, M. D., Mohammed Rezaul, K., & Azizur Rahman, M. (2010). Credit Fraud Detection in the Banking Sector in UK: A Focus on E-Business. *2010 Fourth International Conference on Digital Society*, 234.

Rambola, R., Prateek Varshney, & Prashant Vishwakarma. (2018). Data Mining Techniques for Fraud Detection in Banking Sector. *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 1.

Ray, S. (2019). A Quick Review of Machine Learning Algorithms. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con)*, 35-39.

Sadgal, Sael, & Benabbou. (2019). Performance of machine learning techniques in the detection of financial frauds. *Second International Conference on Intelligent Computing in Data Sciences (ICDS 2018)*, 46.

Xian, L. (2010). Artificial Intelligence and Modern Sports Education Technology. *Huangshi Institute of Technology*, 772-776.

Zamini, M., & Gholamali Montazer. (2018). Credit Card Fraud Detection using autoencoder. *2018 9th International Symposium on Telecommunications (IST'2018)*, 486-491.

Llerena Martinez, G. A., & Terrones Okamura, C. R. (2018). El Design Thinking aplicado en el desarrollo de un Sistema de Información, que permite incrementar la satisfacción de los operarios al reducir los tiempos de atención de Capital Humano. 43.

Visanet. (2015). Visa Business School - Manual del Participante. *Prevención de Fraudes*, 10.

Instituto de Auditores Internos de España. (2015). Manual de Gestión del Riesgo del Fraude. *Prevención, Detección e Investigación*, 17.

Área de Prevención de Fraudes. (2020). Reporte de SPTF del Banco Peruano.

Área de Prevención de Fraudes. (2020). Reportes Internos del Banco Peruano. *Reporte de Reclamos*.

Área de Prevención de Fraudes. (2020). Reportes Internos del Banco Peruano - Importes y cantidad de fraudes por ECI7.

Martin Hernández, S. (2015). Near real time fraud detection with Apache Spark. *Ecole Polytechnique de Bruxelles*, 15.

Narayana , P. (2018). *Udemy*. Obtenido de Spark ML Pipeline Stages like String Indexer, One Hot Encoder and Vector Assembler is used for Pre-processing: <https://www.udemy.com/course/real-time-creditcard-fraud-detection-using-spark/learn/lecture/12456778#overview>

# BIBLIOGRAFÍA

Diario Gestión (3 de marzo de 2020). El 41% de empresas peruanas afirman haber sido víctima de fraude en últimos 2 años. Sección Economía. <https://gestion.pe/economia/el-41-de-empresas-peruanas-afirma-haber-sido-victima-de-fraude-en-ultimos-dos-anos-noticia/>

Digital Security (25 de abril de 2019). Las pérdidas por robo y fraude online ascendieron a 2.700 millones en 2018. Sección EndPoint. <https://www.itdigitalsecurity.es/endpoint/2019/04/las-perdidas-por-robo-y-fraude-online-ascendieron-a-2700-millones-en-2018>

Cámara Peruana de Comercio Electrónico (2019). Ecommerce Perú 2019. Cuál es la tendencia de crecimiento para este año. Sección Prensa. <https://www.capece.org.pe/ecommerce-peru-2019-como-nos-fue-este-ano/>

Lau Carrillo, L. A. (2018). El Design Thinking y la Creatividad en los estudiantes del curso taller de diseño III de la carrera de diseño de interiores en una escuela superior técnica de Lima. 38.

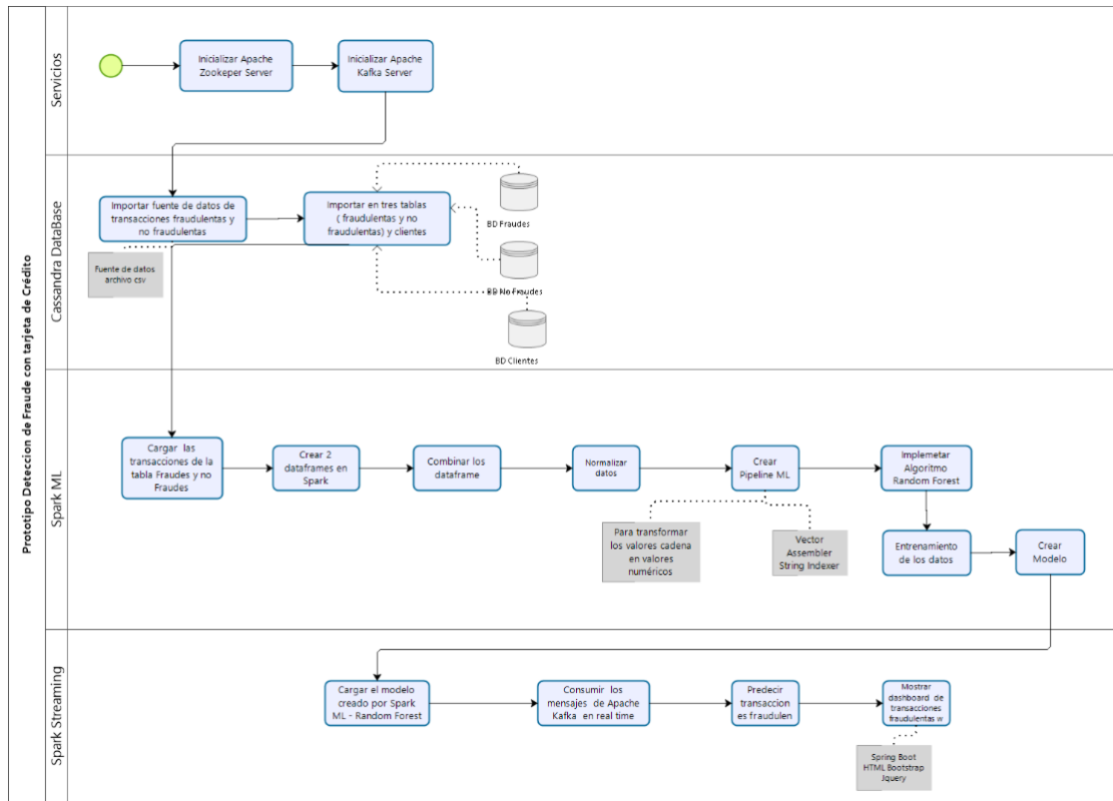
Lan, H., & Pan, Y. (2019). A Crowdsourcing Quality Prediction Model Based On Random Forest. *School of Computer Science Community University of China*, 315-319.

Cama, E (08 de abril de 2020). COVID-19 y la Ciberseguridad. Sección Ciberseguridad. [https://www.ey.com/es\\_pe/cybersecurity/covid-19-la-ciberseguridad](https://www.ey.com/es_pe/cybersecurity/covid-19-la-ciberseguridad)

## ANEXOS

### **Anexo 1 : Flujo de procesos del prototipo desarrollado**





## Anexo 2 : Código fuente - Entrenamiento Algoritmo Random Forest

```
object FraudDetectionTraining extends SparkJob( appName = "Balancing Fraud & Non-Fraud Dataset"){
| val logger = Logger.getLogger(getClass.getName)

def main(args: Array[String]) :Unit {
  Config.parseArgs(args)
  import sparkSession.implicits._

  val fraudTransactionDF = DataReader.readFromCassandra(CassandraConfig.keyspace, CassandraConfig.fraudTransactionTable)
  | .select( col = "cc_num" , cols = "category", "merchant", "distance", "amt", "age", "is_fraud")

  val nonFraudTransactionDF = DataReader.readFromCassandra(CassandraConfig.keyspace, CassandraConfig.nonFraudTransactionTable)
  | .select( col = "cc_num" , cols = "category", "merchant", "distance", "amt", "age", "is_fraud")

  val transactionDF = nonFraudTransactionDF.union(fraudTransactionDF)
  transactionDF.cache()

  transactionDF.show( truncate = false)

  val coloumnNames = List("category", "merchant", "distance", "amt", "age")

  val pipelineStages = BuildPipeline.createFeaturePipeline(transactionDF.schema, coloumnNames)
  val pipeline = new Pipeline().setStages(pipelineStages)
  val preprocessingTransformerModel = pipeline.fit(transactionDF)

  val featureDF = preprocessingTransformerModel.transform(transactionDF)
```

## Anexo 3 :Código fuente - entrenamiento algoritmo Random Forest (separación de data de prueba y validación)

```
val featureDF = preprocessingTransformerModel.transform(transactionDF)

featureDF.show( truncate = false)

val Array(trainData, testData) = featureDF.randomSplit(Array(0.8, 0.2))

val featureLabelDF = trainData.select( col = "features", cols = "is_fraud").cache()

val nonFraudDF = featureLabelDF.filter( condition = $"is_fraud" === 0)

val fraudDF = featureLabelDF.filter( condition = $"is_fraud" === 1)
val fraudCount = fraudDF.count()

println("fraudCount: " + fraudCount)
```

## Anexo 4: Código fuente – Matriz de Confusión

```
val balancedNonFraudDF = DataBalancing.createBalancedDataframe(nonFraudDF, fraudCount.toInt)

val finalfeatureDF = fraudDF.union(balancedNonFraudDF)

val randomForestModel = Algorithms.randomForestClassifier(finalfeatureDF)
val predictionDF = randomForestModel.transform(testData)
predictionDF.show( truncate = false)

val predictionAndLabels =
  predictionDF.select(col( colName = "prediction"), col( colName = "is_fraud").cast(DoubleType)).rdd.map {
    case Row(prediction: Double, label: Double) => (prediction, label)
  }.cache()

val tp = predictionAndLabels.filter { case (predicted, actual) => actual == 1 && predicted == 1 }.count().toFloat
val fp = predictionAndLabels.filter { case (predicted, actual) => actual == 0 && predicted == 1 }.count().toFloat
val tn = predictionAndLabels.filter { case (predicted, actual) => actual == 0 && predicted == 0 }.count().toFloat
val fn = predictionAndLabels.filter { case (predicted, actual) => actual == 1 && predicted == 0 }.count().toFloat
```

## Anexo 5: Código fuente – Matriz de Confusión

```
printf(s"=====  
#####| %-15s          %-15s  
-----+-----  
| Predicted = 1| %-15f          %-15f  
| Predicted = 0| %-15f          %-15f  
|=====  
""", stripMargin, "Actual = 1", "Actual = 0", tp, fp, fn, tn)

println()

val metrics =new MulticlassMetrics(predictionAndLabels)

println("True Positive Rate: " + tp/(tp + fn) // tp/(tp + fn)

println("False Positive Rate: " + fp/(fp + tn)

println("Precision: " + tp/(tp + fp))

randomForestModel.save(SparkConfig.modelPath)
preprocessingTransformerModel.save(SparkConfig.preprocessingModelPath)
```

## Anexo 6: Código fuente – Algoritmo Random Forest

```
import org.apache.spark.ml.classification.RandomForestClassifier
import org.apache.spark.sql.SparkSession
import org.apache.log4j.Logger

object Algorithms {

  val logger = Logger.getLogger(getClass.getName)

  def randomForestClassifier(df: org.apache.spark.sql.DataFrame)(implicit sparkSession: SparkSession) : RandomForestClassificationModel = {
    import sparkSession.implicits._
    val randomForestEstimator = new RandomForestClassifier().setLabelCol("is_fraud").setFeaturesCol("features").setMaxBins(700)
    val model = randomForestEstimator.fit(df)
  }
}
```

## Anexo 7: Código fuente – Visor de Transacciones Fraudulentas

```
<html>
<head>
  <title>Fraud Alert Monitoring Dashboard</title>
  <link rel="stylesheet" type="text/css" href="css/bootstrap.min.css">
  <link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
  <div class="container-fluid">
    <div class="row">
      <div class="col-md-12">
        <h2 class="text-center">
          Sistema de Deteccion de Fraudes por Internet
        </h2>
      </div>
    </div>
    <br>
    <div class="row">
      <!--<div class="col-md-12">-->
      <div class="table-responsive-lg">
        <table class="table table-bordered table-condensed table-hover outerTable">
          <thead>
            <tr>
              <th>NUMERO DE TARJETA</th>
              <th>HORA TRANSACCION</th>
              <th>MOTO/ECI</th>
              <th>MCC</th>
              <th>NOMBRE COMERCIO</th>
              <th>MONTO</th>
              <th>RIESGO VAA</th>
              <th>EDAD</th>
            </tr>
          </thead>
          <tbody>
            <tr>
              <td>
                <div id="fraud_alert">
                  <table class="table table-bordered table-condensed table-hover innerTable">
                    <thead>
                      <tr>
                        <th></th>
                      </tr>
                    </thead>
                    <tbody>
                      <tr>
                        <td></td>
                      </tr>
                    </tbody>
                  </table>
                </div>
              </td>
            </tr>
          </tbody>
        </table>
      </div>
    </div>
  </div>
</body>
</html>
```

## Anexo 8: Código fuente – Visor de Transacciones Fraudulentas

```
<td>
  <div id="fraud_alert">
    <table class="table table-bordered table-condensed table-hover innerTable">
      <tr>
        <thead>
        </thead>
      </tr>
    </table>
  </div>
</td>
</tr>
</tbody>
</table>
</div>
</div>
</div>
</div>
<script type="text/javascript" src="js/jquery-1.12.4.min.js"></script>
<script type="text/javascript" src="js/sockjs-1.1.1.min.js"></script>
<script type="text/javascript" src="js/stomp.min.js"></script>
<script type="text/javascript" src="js/bootstrap.min.js"></script>
<script type="text/javascript" src="js/Chart.min.js"></script>
<script type="text/javascript">
```