
# Desarrollo de herramienta de monitoreo de tráfico LDI para prevención y notificación de fraudes en operadora de telefonía móvil

Freire Conrado, Anthony Bryan

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gestión de Sistemas de Información e Inteligencia de Negocios

Trabajo de titulación previo a la obtención del título de Magíster en Gestión de Sistemas de Información e Inteligencia de Negocios

Mtr. López Davila, Jonathan Fabricio

20 de junio de 2021

Curiginal

## Document Information

| | |
|---|---|
| **Analyzed document** | TRABAJO DE TITULACION ANTHONY FREIRE MAESTRIA 2021 URK.pdf (D109873591) |
| **Submitted** | 6/29/2021 2:07:00 AM |
| **Submitted by** | Diego Marcillo Parra |
| **Submitter email** | dmmarcillo@espe.edu.ec |
| **Similarity** | 1% |
| **Analysis address** | dmmarcillo.espe@analysis.urkund.com |

## Sources included in the report

| | | |
|---|---|---|
| SA | **Universidad de las Fuerzas Armadas ESPE / TesisFinal_FabianOrellana.docx**<br>Document TesisFinal_FabianOrellana.docx (D79194781)<br>Submitted by: frorellana3@espe.edu.ec<br>Receiver: vcparraga.espe@analysis.urkund.com | 3 |
| W | URL: http://repositorium.sdum.uminho.pt/bitstream/1822/65461/1/Dissertacao%252B35974.pdf<br>Fetched: 6/29/2021 2:08:00 AM | 1 |
| SA | **VERSION FINAL.docx**<br>Document VERSION FINAL.docx (D63559390) | 1 |
| W | URL: https://docplayer.es/451618-Escuela-politecnica-nacional.html<br>Fetched: 7/9/2020 6:23:02 PM | 1 |

Firmado electrónicamente por:
JONATHAN FABRICIO LOPEZ DAVILA

---

Ing. Jonathan Fabricio Lopez Davila Mtr.

DIRECTOR

**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

**CENTRO DE POSGRADOS**

# CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Desarrollo de herramienta de monitoreo de tráfico LDI para prevención y notificación de fraudes en operadora de telefonía móvil**" fue realizado por el señor **Freire Conrado, Anthony Bryan** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 20 de junio de 2021

Firma:

JONATHAN FABRICIO LOPEZ DAVILA

Ing. López Dávila, Jonathan Fabricio Mtr.

Director

C.C.: 1716868904


**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

**CENTRO DE POSGRADOS**

## RESPONSABILIDAD DE AUTORÍA

Yo **Freire Conrado, Anthony Bryan**, con cédula de ciudadanía n°1726046350, declaro que el contenido, ideas y criterios del trabajo de titulación: **Desarrollo de herramienta de monitoreo de tráfico LDI para prevención y notificación de fraudes en operadora de telefonía móvil** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

**Sangolquí, 20 de junio de 2021**

Firma (s)

Freire Conrado, Anthony Bryan

**C.C.:** 1726046350


**VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

**CENTRO DE POSGRADOS**

## AUTORIZACIÓN DE PUBLICACIÓN

Yo **Freire Conrado, Anthony Bryan** con cédula de ciudadanía n°1726046350, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Desarrollo de herramienta de monitoreo de tráfico LDI para prevención y notificación de fraudes en operadora de telefonía móvil** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

**Sangolquí, 20 de junio de 2021**

Firma

Freire Conrado, Anthony Bryan

C.C.: 1726046350

**Agradecimiento**

A mi familia por su infinita sabiduría y apoyo a lo largo de mi carrera estudiantil como profesional.

A mi tutor y amigo que día a día me formó humana como profesionalmente para lograr mis metas académicas y laborales.

Anthony.

**Dedicatoria**

A mis padres Mónica y Edwin por su infinito apoyo incondicional que cada día me hacen esforzarme por ser un mejor hijo y hombre de bien para la sociedad. Siempre apoyando mis decisiones y nunca dejándome caer frente a las adversidades. A mi hermano que siempre me apoya con sus risas y ocurrencias que alegran mi vida y la llenan de color. Con esto voy demostrándole quien soy y quiero que este orgulloso de mí.

A mi abuelita Delia que siempre alegra mi día solo con su presencia en mi vida, le doy gracias por haber sido un pilar fundamental en mi crecimiento y espero tenerte muchos años más conmigo. A mi abuelito que, aunque no esté conmigo aun siento la fuerza de su apoyo y todo el amor que me brindo en mi vida, sin ti no podría ser nadie en este mundo y espero que estés orgulloso de mi ya que te dedico todo mi esfuerzo y pasión por la tecnología.

A Jonathan que supo formarme de la mejor manera como coordinador y que me enseñó a crecer más y más en lo académico y laboral, el confió en mí desde que nos conocimos y forjamos más allá del compañerismo una grata amistad.

A mi jefe Diego que siempre me anima a ser una mejor persona y un mejor ingeniero con sus consejos, enseñanzas y, sobre todo, ejemplo. Sin olvidarme de mis compañeros Andrés y Priscila que forman parte de mi vida y siempre han sido gratos en impartirme su conocimiento.

Anthony.

**Índice de Contenido**

## Índice de Tablas

## Índice de Figuras

**Resumen**

Las llamadas de Larga Distancia Internacional representan una gran cantidad de tráfico generado en la actualidad para las operadoras de telefonía móvil; estas generan grandes volúmenes de datos que deben ser monitoreados por especialistas en tiempo real. El monitoreo de tráfico de estas llamadas exige controles exhaustivos por el personal y requiere un conjunto de habilidades basadas en conocimientos teóricos y empíricos. Las llamadas de larga distancia son originadas por la operadora origen y por medio de un Carrier internacional son redireccionadas a todos los países del mundo. Los costes de interconexión son ganancias para las operadoras móviles, actualmente existen defraudadores que buscan estafar para generar ingresos propios o para terceros, que repercuten en pérdidas económicas a la empresa y generan un perjuicio a los abonados.

Las herramientas de monitoreo en la actualidad representan un gran gasto en el presupuesto de las operadoras móviles, por lo que el desarrollo y el uso de herramientas propietarias son una gran apuesta para la reducción de costes, disminución de carga operativa y mitigación y prevención de Fraude LDI.

**Palabras Clave:**

- **LLAMADAS DE LARGA DISTANCIA INTERNACIONAL**
- **TELEFONÍA MÓVIL**
- **MONITOREO DE TRÁFICO**
- **FRAUDE LDI**

**Abstract**

Mobile Long Distance International calls represent a large amount of traffic currently generated for telephone operators; these generate large volumes of data that must be monitored by specialists in real time. Monitoring the traffic of these calls requires extensive controls by staff and requires a skill set based on theoretical and empirical knowledge as well. Long distance calls are originated by the originating operator and through an international Carrier they are redirected to all countries in the world. Interconnection costs are gains for mobile operators, currently there are fraudsters who seek swindle to generate their own income or for third parties, which affect economic losses to the company and generate damage to clients.

Monitoring tools currently represent a large expense in the budget of mobile operators, so the development and use of proprietary tools are a great bet for reducing costs, reducing operational load and mitigating and preventing LDI fraud.

**Keywords:**

- **LONG DISTANCE INTERNATIONAL CALLS**
- **MOBILE TELEPHONY**
- **TRAFFIC MONITORING**
- **LDI FRAUD**

# Introducción

## Antecedentes

Desde el inicio de las comunicaciones móviles, se ha intentado lograr por todas las operadoras del mundo una conexión global, con la finalidad de acortar las distancias de las personas por medio de una llamada de larga distancia. Las operadoras de telefonía móvil de Ecuador se han basado en esta necesidad para ofertar servicios de llamadas a diferentes países en todo el mundo por lo que es necesario destinar recursos de talento humano, infraestructura y software para ofrecer una experiencia de calidad al cliente.

Las empresas de telecomunicaciones han venido trabajando en controles de fraudes con distintas casuísticas, estos se basan en el uso de estrategias e implementación de procesos de aseguramiento de ingresos mediante softwares de monitoreo de llamadas (Humberto & Bermudez, 2019). El incremento de abonados en las operadoras de telefonía móvil en el Ecuador ha generado una mayor captación de posibles víctimas que pueden caer en diferentes tipos de estafas o fraudes sin considerar los grandes costos que estos pueden representar como pérdidas a la economía de la empresa y del cliente.

La gran cantidad de datos generada por el tráfico diario de los abonados representa una dificultad y costo operativo en cuanto se refiere a la detección de fraudes, por lo que los defraudadores se encargan de generar ventaja y lograr beneficios económicos para sus organizaciones delictivas. Las operadoras intentan respaldarse y blindarse ante posibles ataques por lo que se subcontratan sistemas de detección de fraudes a proveedores externos que deben tener una alta disponibilidad debido a que los eventos de fraude ocurren con mayor frecuencia durante los feriados, noches y fines de semana, usualmente cuando las redes se encuentran

menos controladas. Se estima que las telecomunicaciones en el mundo tienen un ingreso promedio anual de 2.30 Trillones de dólares y una pérdida estimada por fraudes de 29.2 Billones de dólares con un porcentaje de pérdida del 1.27% (Mais, Abdallah, & George, 2019).

## Estado del Arte

En este capítulo tratará acerca de la fundamentación teórica para sustentar la presente tesis, se busca tratar elementos relacionados con el tema de estudio, así como documentos y trabajos relacionados. Este capítulo está conformado de la siguiente manera: Planteamiento del problema; Justificación y alcance del proyecto; Revisión de Literatura y Marco Teórico, los mismos que se describen a continuación:

### Planteamiento del problema

La empresa de telecomunicaciones ofrece el servicio de Llamadas de Larga Distancia Internacional (LDI) a sus abonados, se mantendrá el nombre de la empresa como anónima por criterios de seguridad.

En la actualidad la empresa cuenta con un área encargada del control, monitoreo y mitigación de diferentes casuísticas de tráficos de llamadas con comportamientos atípicos. Se presentan diariamente casos de fraudes que pueden generan incidencias en la economía de la empresa y perjuicios económicos en los abonados, por lo que es necesario contar con sistemas de monitoreo de tráfico en tiempo real para el análisis de grandes volúmenes de datos y visualizaciones de indicadores en servidores web.

En base a la implementación de las redes móviles, con el tiempo se vienen realizando convenios con la mayoría de los países de todo el mundo, con la finalidad de generar una conectividad global. Los costos de interconexión con el Carrier Internacional se han ido estableciendo en base a la oferta comercial que se tenga firmada entre las diferentes operadoras de cada país. Existen países que son considerados de riesgo, por el alto costo que presenta realizar una llamada hacia ese destino. Los defraudadores buscan obtener ganancias propias o para

terceros, beneficiándose de estas ofertas comerciales.

La empresa se encuentra vulnerable a los ataques de defraudadores referente a fraudes de llamadas internacionales, esto podría incurrir en grandes pérdidas económicas. Estos eventos pueden llegar a presentar un perjuicio para los clientes lo que afectaría directamente a los NPS (Net Promoter Score) de la empresa y llegar a causar un impacto mediático en el país.

Por estos motivos es necesario el uso de herramientas de monitoreo en tiempo real y con una alta disponibilidad que velen por la seguridad de las llamadas de los abonados, con la finalidad de generar alertas al área de prevención de fraude para que estos incidentes de seguridad puedan ser tratados y mitigados de forma óptima en el menor tiempo posible.

**Justificación y alcance del proyecto**

En la actualidad las operadoras de telefonía móvil registran grandes cantidades de llamadas, los mismos que son enviados hacia el mediador para ser tasados y generar los pagos a las operadoras con las que se tienen convenios de interconexión de llamadas. El gran volumen de datos representa una gran dificultad de obtención y caracterización para los analistas en caso de realizarlo de forma manual. Además, este procedimiento incurre en una carga operativa. El uso de herramientas de monitoreo automático en línea satisface la necesidad del control de fraudes de llamadas de larga distancia internacional. Con la implementación de un software propietario basado en principios de detección y umbrales de fraude, se otorga la capacidad de alertar cuando ocurra un comportamiento atípico de tráfico saliente de Ecuador y además permite disminuir los costos en el presupuesto del área de prevención de fraude.

El presente proyecto pretende extraer los datos de llamadas de forma autónoma y ser

tratados en base a modelos preventivos de fraude establecidos por el administrador del servicio. Existen países que por su alto costo son considerados de riesgo, se realiza una categorización de los destinos en base al costo que se tiene en la oferta comercial de la operadora, cambiando los umbrales de notificación respectivamente con la finalidad de evitar pérdidas económicas a la empresa, se estima que al año existe una pérdida de 29.2 Billones de dólares (Mais , Abdallah , & George , 2019).

Por la casuística de la tipología de fraude que se está tratando, se tienen eventos atípicos en horarios no laborables, fines de semana y feriados, por lo que el sistema debe tener una disponibilidad de 24 horas del día los 365 días del año con la finalidad de generar alertas vía correo electrónico con gráficas en tiempo real hacia el área de prevención de fraude, para que al analista que se encuentra de turno bajo demanda pueda tomar acciones de mitigación y control del incidente, esto debido a que por fraudes en Roaming se puede tener una pérdida por hora de 40.000 euros (Kenigsberg, 2016).

Con los indicadores gráficos que se generan en el web service, se pueden establecer tendencias de tráficos en cada uno de los países que son considerados de riesgo con la finalidad de determinar si es conveniente o no cerrar un destino de forma permanente para que no incurran en más incidentes fraudulentos. Además, se generan correos de información y gráficas dinámicas con periodicidad diaria para poder notificar el estado del tráfico a día caído de las llamadas de larga distancia internacional del Ecuador.

**Revisión de la literatura**

Para el análisis del estado del arte se usaron las fases de criterios de inclusión y estrategia

de búsqueda que son parte de un SMS, como fuentes de búsqueda de la información para la investigación se usaron los siguientes repositorios académicos Scopus, Springer, IEEExplore, ACM Digital Library.

**Definición de los criterios de inclusión y exclusión**

Las bases digitales estudiadas cuentan con una gran cantidad de documentación en base al tema que se esté consultando, por lo cual es esencial definir qué características vamos a requerir para cada artículo que será tomado en cuenta para el presente estudio, se toman en cuenta los criterios siguientes.

**Criterios de inclusión**

Los Criterios de Inclusión definidos para la presente revisión sistemática de literatura son los siguientes:

- El artículo describe características respecto a fraudes
- El artículo describe información científica de casuísticas de fraudes
- El artículo posee referencias a procesos de extracción de datos
- El artículo especifica criterios de análisis de datos

**Criterios de exclusión**

Los Criterios de Exclusión definidos para la presente revisión sistemática de literatura son los siguientes:

- Artículos con antigüedad menor al 2010
- Artículos que estén en otro idioma que no sea inglés

**Grupo de control y palabras clave**

Se pretende utilizar las cadenas de búsqueda para establecer artículos que basaron sus estudios en las palabras clave que formarán parte de la investigación, el primer paso para obtener la información estará basado en varios repositorios con la finalidad de realizar una comparativa final con otros.

**RQ 2.1. ¿Qué estudios existen en la actualidad sobre diferentes casuísticas de fraudes en llamadas?.** En la Tabla 1 se presentan los 6 estudios fundamentales a los cuales se hicieron referencia con la finalidad de determinar diferentes casuísticas de fraudes.

**Tabla 1**

*Estudios por grupo de control*

| No. | Estudio | Palabras clave |
|---|---|---|
| EC1 | Subscription fraud prevention in telecommunications using fuzzy rules and neural networks | Fraud prevention, Fraud detection, Subscription fraud, Neural networks, Fuzzy rules |
| EC2 | Detection of Wangiri Telecommunication Fraud | Telecommunication, Fraud, Detection, Wangiri, |

| | | |
|---|---|---|
| | Using Ensemble Learning | Data Mining, Machine Learning, Ensemble Learning, Classification |
| EC3 | SoK: Fraud in Telephony Networks | Telephony, Ecosystems, Mobile communication, Security, Telecommunications, Telephone sets, Industries |
| EC4 | Discovery of Fraud Rules for Telecommunications Challenges and Solutions | Telecommunications, Fraud, Rule discovery, Mobile communication, |
| EC5 | A probabilistic approach to fraud detection in telecommunications | Kullback–Leibler divergence, Latent Dirichlet Allocation, Fraud detection, User profiling, Telecommunications |
| EC6 | Designing an expert system for fraud detection in private | Fraud detection, User modeling, Expert systems, Telecommunications, Data |

| | |
|---|---|
| telecommunications networks | mining applications |

*Nota.* En la tabla se especifican las palabras clave de cada uno de los artículos científicos extraídos de los diferentes repositorios virtuales. Fuente: Propia.

**Cadena de búsqueda**

Para la generación de la cadena de búsqueda se realiza un análisis de mayores ocurrencias de las palabras y se obtiene un consolidado de las palabras más usadas en los artículos consultados.

**Tabla 2**

*Estudios por grupo de control*

| **Contexto** | **Palabra clave** | **EC1** | **EC2** | **EC3** | **EC4** | **EC5** | **EC6** | **SUM** |
|---|---|---|---|---|---|---|---|---|
| Tipos de fraudes | Fraud | X | X | | X | X | X | 5 |
| | Wangiri | | X | | | | | 1 |
| | Subscription fraud | X | | | | | | 1 |
| | Fraud Detection | X | X | | | X | X | 4 |
| Ámbito | Telecommunications | | X | X | X | X | X | 5 |
| | Telephony | | | X | | | | 1 |
| | Mobile communication | | | X | X | | | 2 |
| | Security | | | X | | | | 1 |
| Técnicas | Neural networks | X | | | | | | 1 |
| | Data mining | | X | | | | X | 2 |

| | | | |
|---|---|---|---|
| | Ensemble Learning | X | 1 |
| | Machine Learning | X | 1 |

*Nota.* En la tabla se realiza un conteo de las palabras clave de cada uno de los artículos científicos extraídos de los diferentes repositorios virtuales. Fuente: Propia.

Con la identificación de las palabras clave, se establece la cadena de búsqueda con la siguiente estructura:

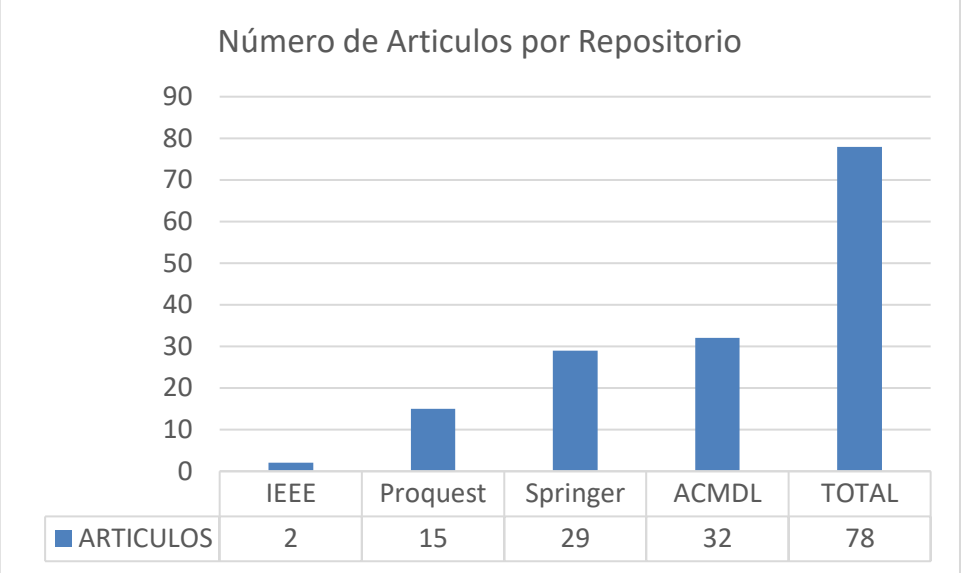
**((Fraud) OR (Fraud Detection)) AND ((Telecommunications) OR (Mobile communication)) AND (Data mining)**

**Proceso de Selección**

En esta etapa se aplica la cadena de búsqueda en los diferentes repositorios académicos con un filtro de fecha no mayor a 10 años de antigüedad.

**Figura 1**

*Cantidad de artículos por repositorio*




*Nota.* La gráfica representa un conteo de los artículos científicos encontrados con la cadena de búsqueda en los diferentes repositorios virtuales. Fuente: Propia.

**Resultados de Revisión**

Con los resultados, se realiza una revisión de los artículos encontrados y en base a su importancia se presenta un resumen de estos.

**RQ 1.2. ¿Cuáles son las técnicas de identificación de fraudes óptimas para la empresa?.** Para la respuesta de esta pregunta de investigación, se realiza un resumen de los estudios fundamentales para la investigación.

**Detection of Wangiri Telecommunication Fraud Using Ensemble Learning** (Mais, Abdallah, & George, 2019)

En el artículo se hace referencia a las innovaciones que se tienen por parte de los

estafadores, lo que hace que la identificación de las técnicas usadas para estafar sea más fácil de detectar. La técnica de fraude Wangiri se destaca por su longevidad, rentabilidad fraudulenta e impacto negativo hacia los abonados y representa uno de los mayores ingresos en los fraudes IRSF. Se tienen miles de millones de transacciones por día realizando fraudes, lo cual representa un problema a escala masiva, proponiendo un gran reto al momento de detectar fraudes efectivos.

**Discovery of Fraud Rules for Telecommunications Challenges and Solutions** (Saharon, Uzi , Einat, Yizhak , & Gadi , 2012)

En el artículo se describe las pérdidas que existen por los fraudes orientados a la industria de las telecomunicaciones, en donde los registros de llamadas no son lo suficiente como para detectar un evento anómalo. Adicionalmente, se hace referencia a cómo los fraudes por suscripción son el principio de eventos de fraudes como las llamadas a servicios premium de alto costo. Existen varias problemáticas al momento de detectar un fraude ya que presenta diferentes tipos de clasificación estándar y problemas de descubrimiento de reglas en otros dominios de minería de datos. Se utilizan algoritmos y métodos para obtener resultados más satisfactorios al momento de la detección de posibles fraudes.

**A probabilistic approach to fraud detection in telecommunications** (Olszewski, 2012)

El autor hace referencia al uso de técnicas de perfilamiento y detecciones de comportamientos fraudulentos basados en clasificaciones de umbrales con el uso de divergencia KL. El método que se propone en el artículo está basado en una clasificación algorítmica que pueden ser solventados a varios problemas, en este caso se hace referencias a detecciones de

fraudes, con el modelo planteado se establece y se propone una descripción acertada del perfil del usuario y puede ser aplicado para solventar problemas en fraudes de telecomunicaciones. Además, este método no requiere de un proceso de entrenamiento de datos, está basado en redes neuronales para realizar la identificación de eventos fraudulentos.

**Designing an expert system for fraud detection in private telecommunications networks** (Constantinos, 2010)

El artículo describe la construcción de un sistema de detección y direccionamiento hacia la detección de casos de fraudes en las redes de telecomunicaciones en organizaciones grandes. Esta herramienta puede ser aplicada a redes similares incorporando únicamente las políticas de privacidad de la red y un conocimiento del manejo de estas. Se usa técnicas de data mining para realizar un monitoreo en las cuentas del usuario, con este análisis y con las pruebas apropiadas, se busca identificar nuevos casos de fraudes. El sistema permite incorporar pruebas en tiempo real en bases de datos históricos.

**Identifying the signs of fraudulent accounts using data mining** (Shing-Han, Yen, Wen-Hui, & Chiang, 2012)

El autor hace referencia principalmente a la severidad que existe en Taiwán respecto a este tipo de fraudes criminales y la gran necesidad que se tiene para detenerlos. Se explica como con el uso de data mining se establecen procesos de exploración útiles, con esta potencial información y características de manejos de grandes cantidades de datos se pueden solventar no solo fraudes de estafas por llamadas telefónicas, sino, fraudes por robos de cuentas bancarias. El objetivo del estudio es explorar e identificar mediante el uso de técnicas de minería de datos, las

transacciones realizadas en los ATM (Automated Teller Machine) bancarios para establecer si existe o no una llamada de algún estafador solicitando datos financieros a los clientes intentando evitar los fraudes.

## Conclusión

Para responder la pregunta de investigación planteada, con las referencias establecidas por los autores, se tienen identificadas las características principales de los fraudes ocurridos alrededor del mundo y se identifica la gran problemática que estas representan tanto para el área de las telecomunicaciones, así como para el área financiera y de bancos. Con los artículos analizados, se tienen varias técnicas orientadas a la revisión de información como minería de datos, big data, análisis de detalles de llamadas, redes neuronales, entre otros. Es por estos motivos que se encuentra una gran importancia en la implementación de controles y notificaciones para optimizar la mitigación de fraudes en la actualidad basándose en técnicas de extracción y análisis de datos de forma masiva.

## Marco Teórico

### Big Data

Actualmente, el avance tecnológico y la creación de nuevas plataformas tecnológicas, entre otros factores, han provocado el crecimiento vertiginoso y voluminosos de los datos, ante lo cual, las empresas han tenido que enfrentarse a nuevos retos que les permitan descubrir, analizar grandes volúmenes de información. A partir de la gran cantidad de datos y la dificultad para manejarlos, surge el término Big Data.

Conforme a un estudio realizado por Cisco, “dos tercios de la población mundial tendrán

acceso a Internet en 2023. Habrá 5.300 millones de usuarios totales de Internet (66 por ciento de la población mundial) en 2023, frente a 3.900 millones (51 por ciento de la población mundial) en 2018. Y, las velocidades 5G serán 13 veces más altas que la conexión móvil promedio para 2023. La velocidad promedio de conexión 5G alcanzará 575 Mbps para 2023" (Cisco, 2020).

Big Data se refiere a la tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la cual es utilizada para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados). Se encuentra caracterizado por las 5 V que componen las dimensiones del big data:

- Volumen. - existe un crecimiento exponencial indeterminado en cuanto a los datos, esta dimensión hace referencia al gran tamaño de información que se maneja en la actualidad en las empresas. Para el uso de estos datos, se requieren del uso de computadores con mejores requerimientos técnicos que los computadores domésticos.

- Velocidad. - a nivel de gestión de datos, el flujo de grandes cantidades de datos aumenta de igual forma, por lo que se deben ir almacenando y tratando los datos con la finalidad de que no existan pérdidas de información.

- Variedad. - existen distintas estructuras y formatos en los que se encuentran los datos, la ventaja del éxito competitivo de una empresa se verá en cómo extraen su información, ya sea como datos estructurados, no estructurados y semi estructurados.

- Veracidad. - con los grandes volúmenes de datos que se extraen, se debe tomar en cuenta cual es la información necesaria y cuál no, el reto en la actualidad es discernir qué datos son útiles para generar conocimiento y cuáles deben ser eliminados debido a que llegan a

ocupar espacio en memoria y procesamiento.

- Valor. - el valor agregado que ofrece la empresa es una de las dimensiones del big data, ya que, gracias a servicios propietarios, las empresas pueden gestionar los datos de mejor manera que la competencia con la finalidad de generar conocimiento.

Del mismo modo, las operadoras móviles son pioneras en manejar grandes volúmenes de información, ya sea en el almacenamiento de registros telefónicos o en la navegación móvil que tiene cada uno de sus usuarios.

**Servicios IIS**

Internet Information Services ofrece un Servidor web flexible y seguro el cual permite subir información de archivos de datos a las aplicaciones web, contando con una alta escalabilidad y una arquitectura abierta, manejado en conjunto con lenguajes de programación .NET o visual Basic. Las principales ventajas que ofrece un servidor generado en IIS son:

- Transporte Estricto de Seguridad HTTP (HSTS) que permite a un sitio web declararse a sí mismo como un host seguro.

- Ofrece implementación de varios host webs al mismo tiempo.

- Presenta mejoras que permiten ejecutar el proceso de trabajo de IIS directamente.

- Ofrece protocolos criptográficos y algoritmos de cifrado para el intercambio de claves y autenticación de mensajes.

**Proceso ETL**

Es un proceso que consta de varios pasos secuenciales que son:

- Extracción: extracción de datos de distintas fuentes como archivos, Excel, páginas web (Infant, Nisha S, Sreemathy, Chaaru, & Gokula, 2020). Existen dos tipos de métodos de extracción:
    - Extracción completa
    - Extracción parcial
        - Con notificación de actualización
        - Sin notificación de actualización
- Transformación: los datos extraídos se encuentran en su forma original y dispuestos de forma no estructurada, por la cual deben ser limpiados, mapeados y transformados. Este paso es importante y clave en el proceso de ETL ya que la correcta limpieza de los datos establecerá la generación de indicadores más efectivos.
- Carga: después de presentar uniformidad en los datos obtenidos, el último objetivo del ETL es cargar los datos en un Data Warehouse, existen 3 tipos de cargas:
    - Carga inicial, se inicializan todas las tablas del Data Warehouse
    - Carga incremental, se aplican cambios progresivos y de escalamiento.
    - Actualización completa, se borra todo el contenido de una tabla y se vuelve a llenar con datos

Después de culminar con estos requerimientos del ETL, se procede a identificar las

posibilidades de generación de conocimiento.

**Simple Mail Transfer Protocol (SMTP)**

SMTP es el protocolo de comunicaciones más utilizado para el servicio de envío de correos electrónicos por internet, el mismo que requiere de una autenticación de usuario y contraseña (Sochor, 2010). Se generan peticiones de conexión desde un cliente hacia el servidor con la finalidad de generar la validación de usuario y el envío de las notificaciones por correos electrónicos con mensajes de texto plano. Para la conexión se destinan IPs dinámicas y puertos de seguridad, para el caso de Gmail son configuradas las siguientes especificaciones:

- Host: smtp.gmail.com
- Puerto: 587
- Habilitación del certificado de seguridad SSL

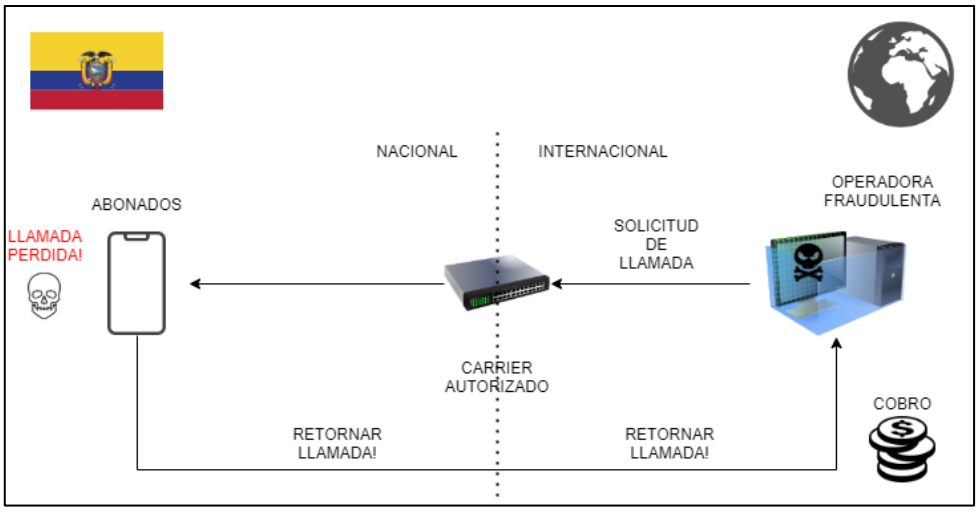
**Fraude Wangiri**

El Fraude Wangiri está orientado a ganar dinero para generar beneficio propio o para terceros. La manera en la que opera este fraude es respecto al uso de bombardeos de llamadas hacia el destino que quiere ser atacado, con la finalidad de que las personas devuelvan la llamada y que se genere un costo por interconexión hacia el destino marcado. Generalmente los países que realizan estas actividades son conocidos por su alto costo de llamada. Los clientes que devuelven las llamadas hacia estos números internacionales escuchan ofertas, o mensajes de publicidad con la finalidad de mantener al abonado la mayor cantidad de tiempo en línea para obtener mayores ganancias para la operadora fraudulenta (Harley , 2014). Existen técnicas de control mediante patrones predictivos de este tipo de casuísticas, las cuales son:

- Volumetría de llamadas entrantes
- Duración de minutos hacia países de alto costo
- Diversidad de números llamando a una misma línea
- Avisos por usuarios externos a la empresa

**Figura 2**

*Diagrama Fraude Wangiri*




*Nota.* El gráfico representa el diagrama de un caso de fraude con tipología Wangiri en el Ecuador. Fuente: Propia

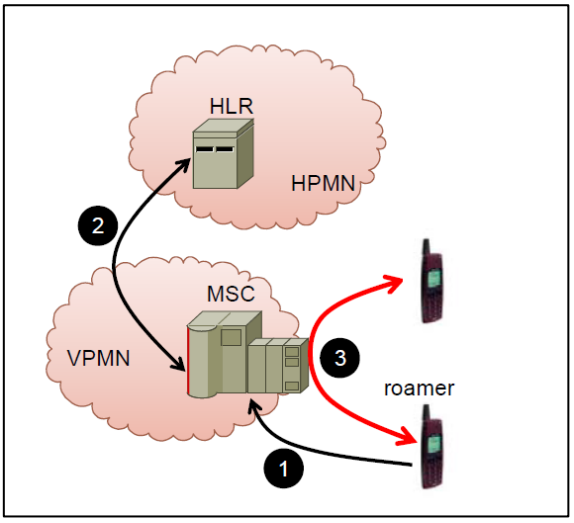
**Fraude Roaming**

En la actualidad y con la globalización de las telecomunicaciones, es necesario encontrarse comunicado en cualquier parte del mundo, por esto, se implementó un sistema que permite hacer uso de la infraestructura de operadoras de cualquier destino por medio del servicio de Roaming Internacional.

Los servicios de Roaming son ofertados por las operadoras de comunicaciones móviles y brindan la ventaja de poder realizar llamadas, mensajes y conexión a internet a sus abonados que se encuentran en otro país. Cuando un abonado se encuentra usando la red de comunicaciones visitante, esta es conocida como VPMN (Visited Public Mobile Network) y esa línea celular pasa a ser conocida como un Roamer out. De igual forma, cuando un abonado se encuentra en la red de operaciones locales HPMN (Home Public Mobile Network) es conocido como un Roamer in.

**Figura 3**

*Escenario de llamada de voz en Roaming*




*Nota.* El gráfico representa el diagrama de una llamada de Roaming Internacional. Tomado de El fraude en roaming: estrategias de ataque y defensa (p.2), por G.M. Fernandez, 2008.

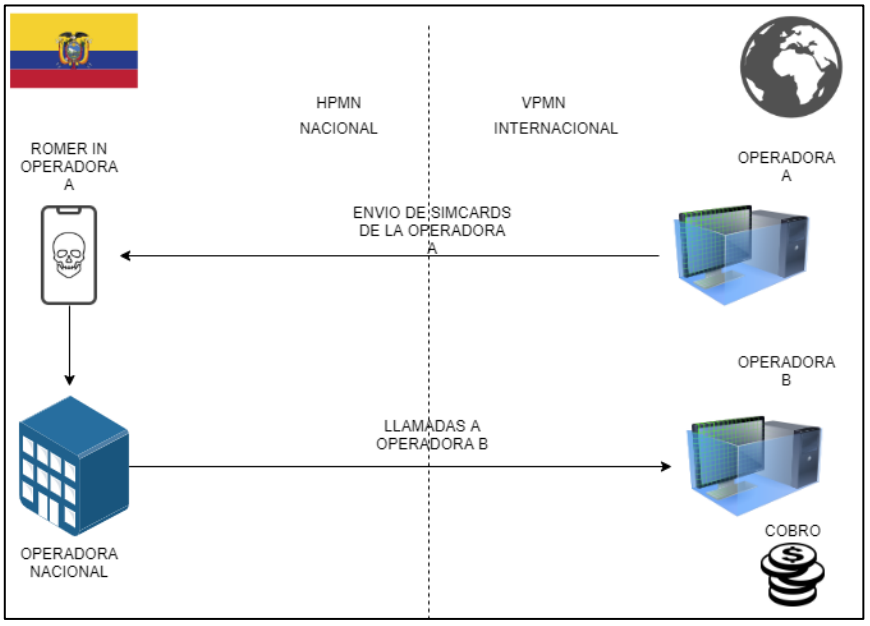
En la Figura 3 se observa el escenario producido por una llamada de voz usando el servicio de Roaming, donde el abonado Roamer in en el punto 1 realiza la solicitud de conexión a la Central de conmutación de la red voz MSC (Mobile Switching Center), después, en el punto 2, la central solicita la validación del servicio activo de Roaming al HLR (Home Location Register) de la

operadora origen el cual almacena los registros de los abonados y sus características para finalmente en el punto 3 realizar la conexión hacia el abonado destino (Gabriel, 2008). Debido a las ofertas comerciales, cada país tiene su acuerdo de roaming con otras operadoras internacionales y manejan sus propias ofertas comerciales, por este motivo el fraude en roaming consiste en aprovechar los altos costos de llamadas de algunos países y generar ganancias. En el total de pérdidas generadas por fraudes, el fraude en Roaming ocupa el 24% de estos valores (Lloyd, 2003). Los defraudadores siguen estos patrones de comportamiento:

- Los defraudadores adquieren simcards de la operadora a la que se va a realizar el fraude.
- Las simcards adquiridas son enviadas hacia el país que brindará el servicio como VPMN.
- Cuando se encuentren los abonados de la operadora visitante registrados en la red y con acceso al servicio de Roaming, se inicia el bombardeo de llamadas hacia destinos de alto costo.
- Los costos generados por las llamadas son cobrados a la operadora origen por la operadora que presta el servicio como VPMN.

**Figura 4**

*Diagrama Fraude Roaming.*




*Nota.* El gráfico representa el diagrama de un escenario de Fraude de Roaming Internacional. Fuente Propia.

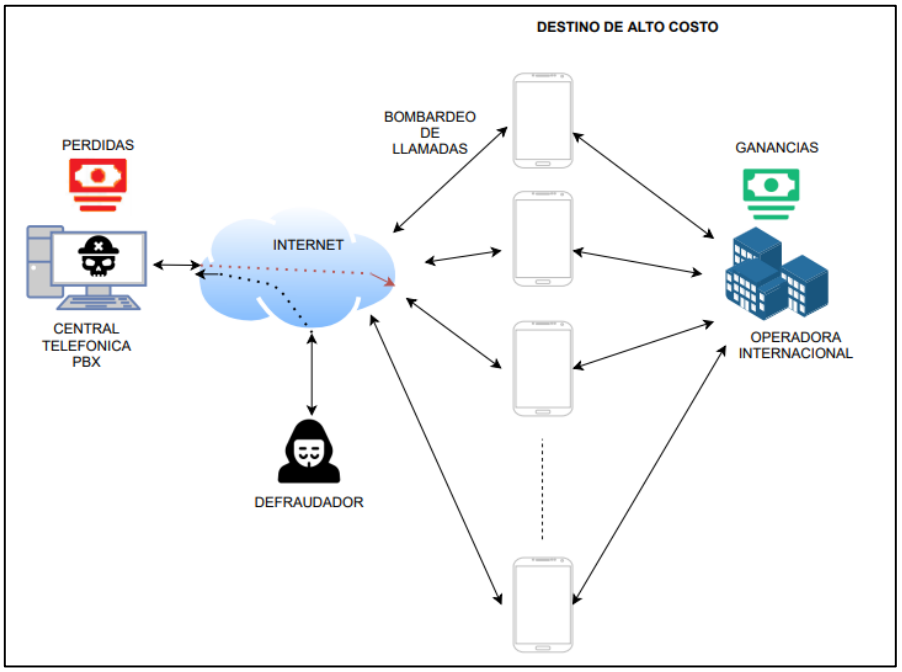
**Fraude hackeo PBX**

Los servicios de centrales telefónicas PBX (Private Branch Exchange) para empresas ha aumentado con la gran demanda de ofertas, requerimientos y necesidades de comunicación para el personal. Estas cuentan con un acceso a internet por el cual salen las llamadas, en base a la seguridad que disponga a nivel de red, puede presentar una brecha hacia estafadores. Los hackeos de centrales telefónicas de empresas han aumentado en la actualidad, el objetivo principal de los ciberdelincuentes es vulnerar las seguridades de la empresa a nivel de red y bombardear de llamadas, a expensas del administrador de la plataforma, hacia destinos de alto costo generando pérdidas a la empresa y donde solo se pondrán en contexto cuando reciban la factura del pago que tienen que realizar . Existen operadoras que financian a los delincuentes para que realicen

sus actos delictivos con la finalidad de generar más tráfico hacia sus operaciones y aumentar las ganancias (Camacho Sellán & González Mora, 2016).

**Figura 5**

*Diagrama Fraude PBX.*




*Nota.* El gráfico representa el diagrama de un escenario de Fraude de PBX. Fuente: Propia.

**Empresas de telecomunicaciones**

En la actualidad las telecomunicaciones han tenido un gran avance tecnológico y un crecimiento abrumador en sus abonados por lo que según datos del INEC (Instituto Nacional de Estadística y Censos) en el año 2018 se tiene un incremento de 8.6 puntos porcentuales a nivel nacional de personas que tienen un teléfono celular activado (INEC, 2018).

Entre los servicios ofertados por las empresas de telecomunicaciones se tienen los siguientes:

- Llamadas de Voz
- Mensajería de texto
- Internet
- Proveedores de servicio de Internet
- Servicios de almacenamiento en la nube
- Servicios de Business Intelligence
- Servicio de televisión digital
- Servicio de telefónica fija

# Metodología de Investigación

En este capítulo se desarrollan las metodologías planteadas para el cumplimiento de los objetivos de la presente tesis. El mismo se encuentra conformado de la siguiente forma: Objetivos General y Específicos; Preguntas de Investigación; Categorización de Variables; y Fases de la Metodología de Investigación. Las mismas se describen a continuación:

## Objetivo general

Desarrollar una herramienta de monitoreo de tráfico LDI mediante técnicas de Business Intelligence para la identificación de potenciales fraudes, con la finalidad de mitigarlos de forma óptima con tiempos de respuesta cortos.

## Objetivos específicos

**OE1:** Realizar un análisis de literatura mediante una revisión inicial, para determinar las casuísticas de fraudes en llamadas internacionales.

**OE2**: Implementar en la empresa la herramienta de monitoreo de tráfico LDI mediante el uso de las metodologías KDD y CRISP-DM.

**OE3**: Evaluar el rendimiento de la herramienta desarrollada mediante el uso de técnicas de inteligencia de negocios.

## Preguntas de Investigación

Para la consecución de los objetivos específicos del proyecto de desarrollo de herramienta de monitoreo de tráfico LDI para prevención y notificación de fraudes se requiere que se respondan las siguientes preguntas:

**RQ para el Objetivo 1**

**RQ1.1:** ¿Qué estudios existen en la actualidad sobre diferentes casuísticas de fraudes en llamadas?

**RQ1.2:** ¿Cuáles son las técnicas de identificación de fraudes óptimas para la empresa?

**RQ para el Objetivo 2**

**RQ2.1:** ¿Cuáles son las fuentes de datos que tiene disponible la empresa respecto a tráfico de voz?

**RQ2.2:** ¿Cuáles son los umbrales de número llamadas y duración total de minutos para la notificación por nivel de criticidad del país?

**RQ para el Objetivo 3**

**RQ3.1:** ¿Qué volumen de datos promedios son extraídos y monitoreados por la herramienta desarrollada?

**RQ3.2:** ¿Cuántos fraudes fueron detectados y mitigados a tiempo con la herramienta desarrollada?

En base a los objetivos planteados y a las preguntas de investigación propuestas, se plantea la hipótesis.

**Hipótesis**

La implementación de una herramienta de monitoreo de tráfico LDI permite identificar y mitigar fraudes en llamadas de manera óptima.

**Hipótesis Alternativa**

La implementación de una herramienta de monitoreo de tráfico LDI no permite identificar y mitigar fraudes en llamadas de manera óptima.

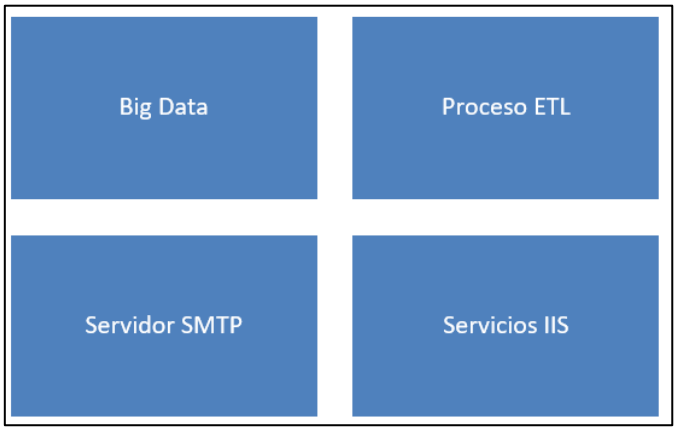
**Categorización de Variables**

**Fundamentación de la Variable Independiente**

Con la finalidad de buscar responder a la hipótesis, se realiza como primera instancia la fundamentación de la variable independiente tomando en cuenta los temas de estudio propuestos bajo la jerarquía presentada en la ilustración 2.

**Figura 6**

*Fundamentación Variable Independiente*



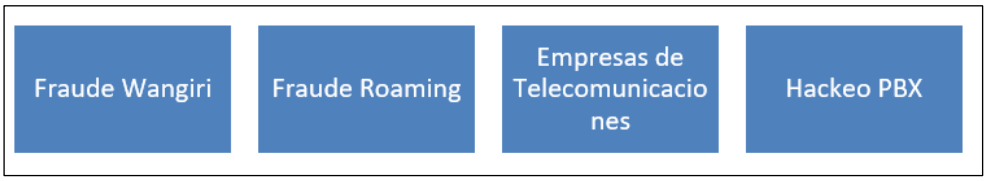

*Nota.* Temas que serán analizados con la variable Independiente. Fuente: Propia.

**Fundamentación de la Variable Dependiente**

Manteniendo la finalidad de buscar responder la hipótesis, se realiza la fundamentación de la variable dependiente tomando en cuenta los temas de estudio propuestos bajo la jerarquía presentada en la Figura 7.

**Figura 7**

*Fundamentación Variable Dependiente*




*Nota.* Temas que son analizados con la variable Dependiente. Fuente: Propia.

**Fases de la Metodología de desarrollo del aplicativo**

La metodología que se implementó es una combinación de las características de Knowledge Discovery in Databases (KDD) y Cross Industry Standard Process for Data Mining (CRISP-DM), lo que implica evaluación de patrones para tomar decisiones, generar conocimiento y evaluar el rendimiento. Se encuentra compuesto por las siguientes etapas:

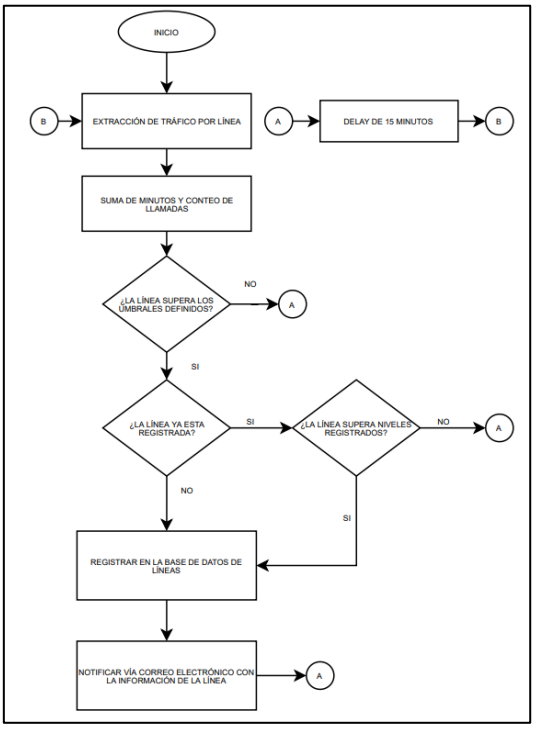
- Selección
- Procesamiento
- Transformación
- Data Mining
- Generación de Conocimiento
- Evaluación de rendimiento

Para la detección de líneas individuales y destinos que presentan tráfico atípico, se establece una lógica de programación basada en los controles manuales que se realizan en la empresa. Dichos controles realizan una revisión permanente y autónoma del tráfico de larga

distancia internacional de la operadora. A continuación, se presenta un flujo de cómo serán las detecciones y notificaciones automáticas para el análisis de líneas individuales.

**Figura 8**

*Diagrama de flujo detección líneas individuales*

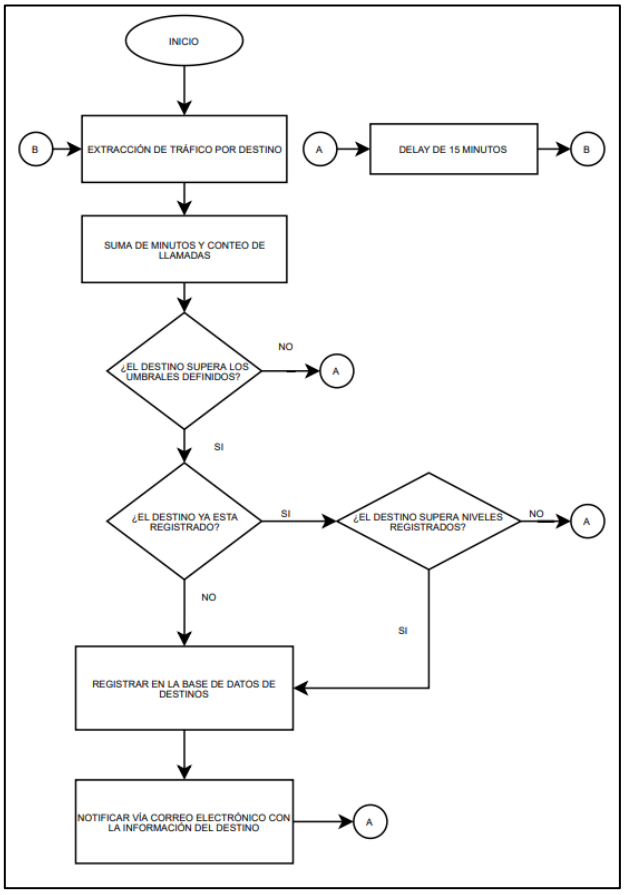



*Nota.* La gráfica representa el diagrama de flujo que seguirá el programa para la detección de posibles fraudes en líneas individuales. Fuente: Propia.

Para el segundo escenario se plantea un control a nivel de parámetros extraídos de cada uno de los destinos internacionales del mundo con la finalidad de observar cada país como un conjunto y poder mitigar posibles fraudes Wangiri eficazmente.

**Figura 9**

*Diagrama de flujo detección Wangiri*




*Nota.* La gráfica representa el diagrama de flujo que seguirá el programa para la detección de posibles fraudes Wangiri. Fuente: Propia.

Los flujos presentados en la Figura 8 y Figura 9 representan el proceso de detección de un evento de fraude, los mismos han sido basados en modelos preventivos de fraude que serán detallados a lo largo de la metodología expuesta en el proyecto.

A continuación, se explicará cada una de las etapas de la metodología en base a los requerimientos para el desarrollo de la herramienta de monitoreo.

# Desarrollo de la Propuesta

En este capítulo se desarrolla de forma teórica la implementación de cada una de las fases de la metodología planteada. El mismo está conformado de la siguiente forma: Selección; Procesamiento; Transformación; Data Mining; Evaluación de rendimiento; Generación de Conocimiento; Resultado Final.

## Selección

### Análisis de tráfico y categorización de destinos

La información histórica, será premisa para categorizar destinos de alto riesgo, sumado a la oferta comercial de interconexión y la experiencia por parte del equipo de fraude. Es importante recalcar que, la GSMA (Global System For Mobile Comunication Association) siendo el ente regulador a nivel internacional de operadores móviles proporciona información de países con alto riesgo, la misma será analizada y acoplada a la categorización del país.

En base a los parámetros anteriormente descritos, se establecen 5 niveles de criticidad para todos los destinos del mundo. Para el caso de la operadora seleccionada se establecerá en la siguiente tabla la cantidad de destinos correspondientes a cada uno de los niveles de riesgo. Adicionalmente, no se definirá el nombre del destino y su nivel correspondiente con la finalidad de evitar que los defraudadores puedan tener acceso a esta información.

**Tabla 3**

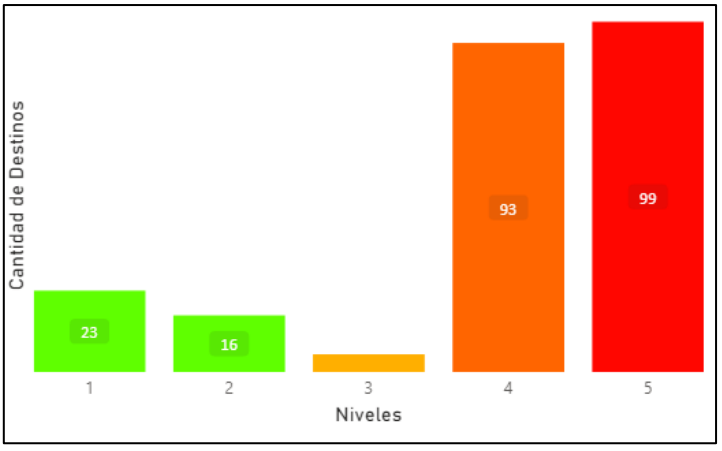
*Cantidad de destinos por nivel de criticidad*

| Niveles | Cantidad de Destinos |
|---|---|
| 1 | 23 |
| 2 | 16 |
| 3 | 5 |
| 4 | 93 |
| 5 | 99 |
| **Total general** | **236** |

*Nota.* La tabla representa la cantidad de destinos a nivel mundial por cada uno de los niveles de criticidad establecidos. Fuente: Propia.

**Figura 10**

*Cantidad de destinos por nivel de criticidad*




*Nota.* La gráfica representa la cantidad de destinos a nivel mundial de acuerdo a cada uno de los niveles de criticidad planteados. Fuente: Propia.

Como se determina en la Figura 7, para el Ecuador la criticidad de los países es sin duda importante, en general podemos determinar que se tiene un 39.41% y 41.95% de destinos con nivel de criticidad 4 y 5 respectivamente, es hacia estos países hacia dónde vamos a centrar el

control automático de tráfico LDI, sin descuidar el control de los otros niveles en busca de posibles nuevos destinos de alto riesgo.

Basándose en patrones predictivos de prevención de fraude, se establecen umbrales de control basados en los siguientes conceptos:

- Cantidad de llamadas hacia el destino
- Duración total de llamadas hacia el destino

Tomando en cuenta los patrones mencionados anteriormente, se establecen los umbrales para cada uno de los niveles de criticidad. Cabe recalcar que en este trabajo de titulación se manejará una nomenclatura encriptada para cada uno de los valores de umbral con el fin de precautelar la información de la empresa y la fuga de información evitando intentos malintencionados de la misma.

Para la mitigación del fraude LDI se procede con la consulta de cada abonado que está realizando llamadas LDI de forma individual, se establecen los siguientes umbrales en base a la criticidad del destino.

**Tabla 4**

*Umbrales de control por nivel de criticidad por abonado*

| Niveles | Cantidad de Llamadas | Duración de Llamadas |
|---|---|---|
| 1 | C1 | D1 |
| 2 | C2 | D2 |
| 3 | C3 | D3 |
| 4 | C4 | D4 |
| 5 | C5 | D5 |

*Nota.* En la tabla se especifican valores que hacen referencia a cada umbral de control individual en el nivel de criticidad del destino. Fuente: propia.

Además, para la mitigación del fraude Wangiri se procede con la consulta en conjunto de todos los destinos del mundo, se establecen los siguientes umbrales en base a la criticidad de este.

**Tabla 5**

*Umbrales de control por nivel de criticidad por destino*

| Niveles | Cantidad de Llamadas | Duración de Llamadas |
|---|---|---|
| 1 | CD1 | DD1 |
| 2 | CD2 | DD2 |
| 3 | CD3 | DD3 |
| 4 | CD4 | DD4 |
| 5 | CD5 | DD5 |

*Nota.* En la tabla se especifican valores que hacen referencia al umbral de control en conjunto basados en el nivel de criticidad del destino. Fuente: propia.

## Procesamiento

### Extracción de datos y generación de información

Se plantean diferentes procesos de consulta que permiten obtener tendencias de tráfico

de llamadas de larga distancia internacional. Las consultas se encuentran desarrolladas en Oracle y están optimizadas debido a que las tablas son de producción y el uso excesivo de procesamiento puede generar indisponibilidad en las bases de datos y detener procesos que se encuentran ejecutándose en paralelo.

Como primer control automático, se generó un query que permite obtener los abonados que superan los umbrales establecidos para cada uno de los destinos en base a los diferentes niveles de criticidad con la finalidad de controlar el fraude de llamadas LDI individualmente. La consulta que se ejecuta a nivel de Oracle es la siguiente:

**Figura 11**

*Consulta por abonado en Oracle*

```
select /*+parallel (a,16)full(a)*/ a.NumeroA, count(a.NumeroA) llamadas,
ceil(sum(a.Duracion)/60) as duracion, a.destino
from registros_llamadas_LDI a
where a.Fecha_Inicio between sysdate-1 and sysdate
and a.destino in (select b.nombre_destino
from Destinos_mundo b
where b.codigos_destino in ("códigos de área por destino"))
group by a.NumeroA, a.destino
having
--Definición de Umbrales por criticidad de destino:
((count(NumeroA) > C1 and ceil(sum(duracion_num)/60) > D1)
and a.destino in ("códigos de área destinos de nivel 1"))
or ((count(NumeroA) > C2 and ceil(sum(duracion_num)/60) > D2)
and a.destino in ("códigos de área destinos de nivel 2"))
or ((count(NumeroA) > C3 and ceil(sum(duracion_num)/60) > D3)
and a.destino in ("códigos de área destinos de nivel 3"))
or ((count(NumeroA) > C4 and ceil(sum(duracion_num)/60) > D4)
and a.destino in ("códigos de área destinos de nivel 4"))
or ((count(NumeroA) > C5 and ceil(sum(duracion_num)/60) > D5)
and a.destino in ("códigos de área destinos de nivel 5"))
```

*Nota.* Se detalla la consulta del consumo de minutos y cantidad de llamadas de los abonados hacia destinos internacionales. Fuente: propia.

De igual forma, como se requiere una visión general de los destinos con la finalidad de mitigar el fraude con tipología Wangiri, se establece el siguiente query de consulta en Oracle:

**Figura 12**

*Consulta por destino en Oracle*

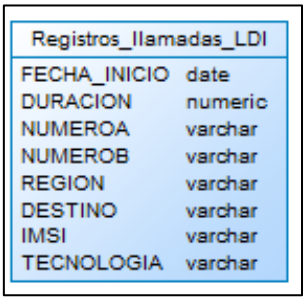
```
select /*+parallel (a,16)full(a)*/ count(a.NumeroA) llamadas,
ceil(sum(a.Duracion)/60) as duracion, a.Destino, b.codigo_destino
from registros_llamadas_LDI a, Destinos_mundo b
where  a.fecha_inicio between sysdate-1
and sysdate
and a. Destino = b.nombre_destino
and b.codigo_destino in ("códigos de área por destino")
group by a.destino,b.codigo_ destino
having
--Definición de Umbrales por criticidad de destino:
((count(telefono_origen) > CD1 or ceil(sum(duracion_num)/60) > DD1)
and a. destino in (" códigos de área destinos de nivel 1"))
or ((count(telefono_origen) > CD2 or ceil(sum(duracion_num)/60) > DD2)
and a. destino in (" códigos de área destinos de nivel 2"))
or ((count(telefono_origen) > CD3 or ceil(sum(duracion_num)/60) > DD3)
and a. destino in (" códigos de área destinos de nivel 3"))
or ((count(telefono_origen) > CD4 or ceil(sum(duracion_num)/60) > DD4)
and a. destino in (" códigos de área destinos de nivel 4"))
or ((count(telefono_origen) > CD5 or ceil(sum(duracion_num)/60) > DD5)
and a. destino in (" códigos de área destinos de nivel 5"))
```

*Nota.* Se detalla la consulta del consumo de minutos y cantidad de llamadas de los destinos internacionales. Fuente: propia.

Las dos consultas implementadas para el control de fraude LDI individual y Wangiri, se encuentran consultando información en la base de datos de interconexión, específicamente en las tablas de llamadas internacionales y de registro de países.

**Figura 13**

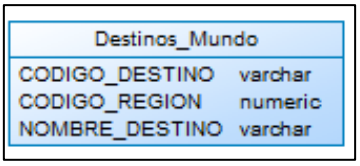
*Diagrama tabla de registros de llamadas LDI*




*Nota.* Diagrama Físico de la tabla de registros de llamadas de LDI . Fuente: Propia.

**Figura 14**

*Diagrama tabla de destinos mundo*




*Nota.* Diagrama Físico de la tabla en la que se registran los destinos del mundo en base a su código de área. Fuente: Propia.

Teniendo en cuenta el uso de estas dos tablas para la extracción de la información, es importante realizar un detalle de cada uno de los campos con los que nos encontramos trabajando en las consultas de Oracle.

**Tabla 6**

*Descripción de los campos por tabla de Llamadas*

| Tabla | Campo | Tipo | Descripción |
|---|---|---|---|
| Registros_Llamadas_LDI | FECHA_INICIO | DATE | Fecha de inicio de la llamada saliente |
| Registros_Llamadas_LDI | DURACION | NUMERIC | Duración de la llamada |

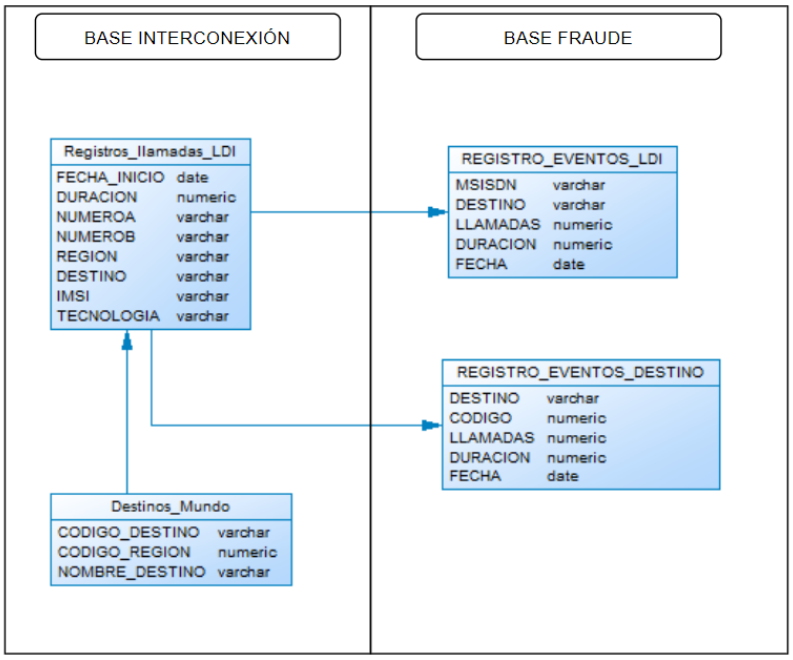
| | | | |
|---|---|---|---|
| Registros_Llamadas_LDI | NUMEROA | VARCHAR | Número que origina la llamada |
| Registros_Llamadas_LDI | NUMEROB | VARCHAR | Número que recepta la llamada |
| Registros_Llamadas_LDI | REGION | VARCHAR | Región en la que se encuentra el país al que se está llamando |
| Registros_Llamadas_LDI | DESTINO | VARCHAR | Nombre del país al que se está realizando la llamada |
| Registros_Llamadas_LDI | IMSI | VARCHAR | Registro del Código de identificación del teléfono móvil que originó la llamada |
| Registros_Llamadas_LDI | TECNOLOGIA | VARCHAR | Tecnología de comunicación en la que se encuentra realizando la llamada |
| Destinos_Mundo | CODIGO_DESTINO | VARCHAR | Código telefónico asignado a cada destino del mundo |
| Destinos_Mundo | CODIGO_REGION | NUMERIC | Código de registro de la región del destino al que se está generando la llamada |
| Destinos_Mundo | NOMBRE_DESTINO | VARCHAR | Nombre del país al que se está realizando la llamada |

*Nota.* En la tabla se encuentra la descripción de cada uno de los campos que van a ser usados para las consultas en Oracle. Fuente: Propia.

Al tener información en dos bases de datos diferentes, se crea el modelo entidad relación entre la base de datos de interconexión y la base de datos de fraude como se muestra en la Figura 15.

**Figura 15**

*Diagrama entidad relación base de datos*




*Nota.* En la figura se muestra el diagrama entidad relación entre las bases de interconexión y fraude. Fuente: Propia.

**Desarrollo del web service de monitoreo back-end**

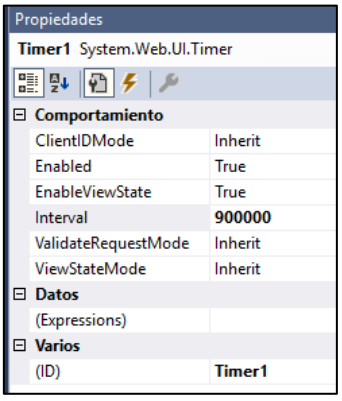
En base al lenguaje de programación de .NET, se implementó un web service de back-end con el modelo vista controlador (MVC) que consultará los datos de forma autónoma con una periodicidad de 15 minutos con la finalidad de extraer el tráfico de llamadas de larga distancia y monitorear su comportamiento basándose en los procesos de consultas creados en el apartado anterior. Este web service será destinado únicamente como motor de análisis que se encuentra ejecutándose en segundo plano.

Como primer punto se crea un timer con el uso de la clase temporizador de visual basic,

la misma está encargada de ejecutar consultas de datos de los servicios web síncronos y asíncronos en un periodo de tiempo determinado (Timer, 2021). Tomando el cuenta el uso de esta clase, se establece un control cada 900000ms que representan el intervalo de tiempo de actualización de la página con la extracción de datos. Las propiedades configuradas en el desarrollo que se encuentran definidas para estas consultas recurrentes son las siguientes:

**Figura 16**

*Propiedades de la clase timer*



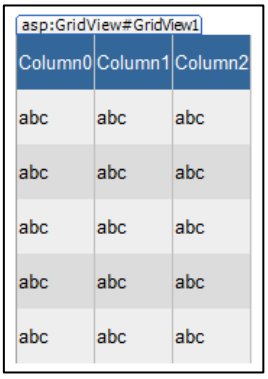

*Nota.* En la gráfica se muestran las propiedades que se encuentran configuradas en el timer.

Fuente: Propia.

Con la finalidad de ir almacenando la información que se obtiene en cada una de las consultas, se crea una rejilla de visualización de datos dinámica (Data Grid View) perteneciente a la clase windows forms (DataGridView, 2021), la misma permite presentar datos ordenados en formato de tabla con columnas y filas auto dimensionadas.

**Figura 17**

*Data Grid View creado*




*Nota.* En la gráfica se muestran la rejilla de visualización de datos para las diferentes funciones programadas. Fuente: Propia.

Con la rejilla de visualización de datos creada, es necesaria primeramente la configuración del tick del timer que representa toda la programación que se ejecuta pasado el tiempo establecido en las propiedades definidas anteriormente.

**Figura 18**

*Programación del tick del timer*

```
Protected Sub Timer1_Tick(sender As Object, e As EventArgs) Handles Timer1.Tick
    GridView1.DataSource = Extraer_Informacion()
    GridView1.DataBind()
    Crearconsulta()
End Sub
```

*Nota.* Descripción de los comandos que ejecuta el tick del timer periódicamente. Fuente: Propia.

El tick está encargado de ejecutar la consulta en las tablas de registro de llamadas y de destino con la finalidad de extraer la información y presentarla en el Data Grid View de forma periódica en base a los parámetros configurados anteriormente como se puede visualizar en la

figura 18.

Para el control de abonados individual y por destino es necesario agregar esta información al Data Grid View con el uso de la función DataSource que recepta un Data_Table con el detalle de filas y columnas. Con el uso de las clases del proveedor de datos de .NET Framework para Oracle denominado System.Data.OracleClient. En base a esta clase, vamos a usar las siguientes funciones:

- Oracle Connection
- ConnectionString
- OracleCommand
- OracleDataAdapter

**Figura 19**

*Programación de la función Extraer Información*

```
Private Function Extraer_Informacion() As DataTable
    Dim cnn_destino As New OracleConnection
    cnn_destino.ConnectionString = ("SERVIDOR;USUARIO;PASSWORD;")
    Dim _SelectTable As String = "QUERY DE CONSULTA"
    Dim datos_base1 As New DataTable()
    Using cmd_destino As New OracleCommand(_SelectTable, cnn_destino)
        Using da As New OracleDataAdapter(cmd_destino)
            Try
                cmd_destino.Connection.Open()
                da.Fill(datos_base1)
                cmd_destino.Connection.Close()
            Catch ex As Exception
            End Try

            Dim cont As Integer
            Dim lineas(datos_base1.Rows.Count) As String
            Dim row As DataRow
            For cont = 0 To datos_base1.Rows.Count - 1 Step 1
                row = datos_base1.Rows(cont)
            Next cont
            cmd_destino.Connection.Close()
        End Using
    End Using
    Return datos_base1
End Function
```

*Nota.* Programación de la función que ejecuta las consultas a las tablas generadas anteriormente. Fuente: Propia.

**Tabla 7**

*Descripción de los variables de la función extraer información*

| Variable | Namespace | Descripción |
|---|---|---|
| cnn_destino | OracleConnection | Variable que almacena los parámetros de conexión de la base de datos |
| _SelectTable | String | Variable que contiene el query de consulta a ejecutarse |
| datos_base1 | DataTable | Tabla en la cual se almacenan las consultas realizadas en Oracle |
| cont | Integer | Variable numérica incremental con la cantidad de filas consultas |

| | | |
|---|---|---|
| lineas | String | Arreglo dinámico de cadenas de texto con las líneas telefónicas consultadas |
| row | DataRow | Variable que almacena las filas que fueron consultadas en Oracle |

*Nota.* La tabla describe cada una de las variables usadas en la función para extraer información.

Fuente: Propia.

**Transformación**

**Limpieza de datos**

La información que se encuentra en la base de datos de llamadas internacionales contiene parámetros relevantes y no relevantes para el estudio, en esta etapa se limitarán los campos extraídos con la finalidad de que se tenga la tabla de forma estructurada con valores importantes que permitan generar patrones de detección de fraudes.

Con la finalidad de limpiar la información que se obtiene de cada una de las extracciones de tráfico de la red, se toman en cuenta las siguientes correcciones:

- Eliminación de registros de llamadas duplicadas
- Eliminación de registros con llamadas nulas
- Eliminación de registros de llamadas incompletos

Después de realizar este proceso de limpieza, se cargan los datos hacia el data grid view implementado en el web service, el mismo que permite generar columnas y filas de forma dinámica. En esta tabla se registran todos los eventos que se encuentren superando el umbral

predefinido para cada uno de los destinos o de los abonados de forma individual como se muestra en la figura 19.

**Figura 20**

*Data Grid View dinámico con información*

| LLAMADAS | DURACION | PAIS | CODIGO_PAIS |
|---|---|---|---|
| 31 | 1300 | ESPAÑA | +34 |
| 29 | 256 | MARRUECOS | +212 |
| 145 | 20 | NICARRAGUA | +505 |

*Nota.* En la figura se encuentra un ejemplo de un Data Grid View con información extraída de las tablas de consulta de tráfico LDI. Fuente: Propia.

**Data Mining**

**Patrones de Comportamiento**

Los modelos preventivos de fraude permiten implementar patrones predictivos de comportamiento de llamadas de larga distancia internacional son utilizados para detectar tráficos anómalos e irregulares, los mismos se encuentran basados en:

- Países de Alto Riesgo
- Cantidad de llamadas Salientes durante un periodo de tiempo determinado
- Duración de llamadas Salientes durante un periodo de tiempo determinado

Los números telefónicos que presenten un tráfico atípico con comportamiento de Fraude LDI y Wangiri son almacenados en la base de datos creada exclusivamente para el área de

prevención de fraude, con la finalidad de tener registrados todos los eventos y con los siguientes datos informativos:

- Número de la línea (MSISDN) que está realizando el alto consumo de llamadas
- País de destino al que se están realizando las llamadas
- Cantidad de llamadas realizadas durante las últimas 24 horas
- Duración de las llamadas realizadas durante las últimas 24 horas
- Fecha de detección

Los eventos que serán detectados por la herramienta son los siguientes:

- Números telefónicos prepago
- Números telefónicos con planes pospago
- Números telefónicos de otros países (Roamers in)
- Números telefónicos con planes Siptrunk
- Destinos internacionales

**Almacenamiento de eventos**

Después de realizar todo el proceso de detección y limpieza de datos, es necesario almacenar los eventos generados con la finalidad de llevar un registro histórico de los posibles destinos y líneas con comportamientos atípicos de tráfico con patrones de fraude.

Se implementan dos tablas en la base de datos de Oracle que permiten almacenar de forma diferenciada los abonados con la finalidad de registrar fraudes LDI y los destinos con la finalidad de registrar fraudes Wangiri. Las dos tablas creadas son:

- REGISTRO_EVENTOS_LDI
- REGISTRO_EVENTOS_DESTINOS

**Figura 21**

*Tablas de registro Fraude*


*Nota.* En la figura se encuentra el diagrama de las tablas en Oracle que almacenan los eventos de abonados y de destinos para cada tipología de fraude. Fuente: Propia.

**Tabla 8**

*Descripción de los campos por tabla de registros*

| Tabla | Campo | Tipo | Descripción |
|---|---|---|---|
| REGISTRO_EVENTOS_LDI | MSISDN | VARCHAR | Número de línea del abonado que se encuentra realizando llamadas con tráfico atípico |
| REGISTRO_EVENTOS_LDI | DESTINO | VARCHAR | Nombre del país al que se está realizando las llamadas |
| REGISTRO_EVENTOS_LDI | LLAMADAS | NUMERIC | Conteo de las llamadas distintas que tiene el abonado hacia el destino |

| | | | |
|---|---|---|---|
| REGISTRO_EVENTOS_LDI | DURACION | NUMERIC | duración total de las llamadas del abonado hacia el destino |
| REGISTRO_EVENTOS_LDI | FECHA | DATE | Fecha en la que se registró el tráfico irregular del abonado |
| REGISTRO_EVENTOS_DESTINOS | DESTINO | VARCHAR | Nombre del país al que se está realizando las llamadas |
| REGISTRO_EVENTOS_DESTINOS | CODIGO | NUMERIC | Código de área del destino al que se están realizando las llamadas |
| REGISTRO_EVENTOS_DESTINOS | LLAMADAS | NUMERIC | Conteo de todas las llamadas distintas que se están generando hacia el destino |
| REGISTRO_EVENTOS_DESTINOS | DURACION | NUMERIC | duración total de las llamadas hacia el destino |
| REGISTRO_EVENTOS_DESTINOS | FECHA | DATE | Fecha en la que se registró el tráfico irregular del destino |

*Nota.* En la tabla se encuentra la descripción de cada uno de los campos que van a ser usados para los registros de los eventos en Oracle. Fuente: Propia.

Con las tablas de registros es necesario crear los querys de ejecución para insertar los eventos según los campos creados anteriormente.

**Figura 22**

*Query de registro de eventos individuales*

```
insert into REGISTRO_EVENTOS_LDI
values (MSISDN, DESTINO, LLAMADAS, DURACION, FECHA)
```

*Nota.* En la figura se encuentra el query de registro con los diferentes campos necesarios para los eventos de fraude LDI individual por abonado. Fuente: Propia.

**Figura 23**

*Query de registro de eventos Wangiri*

```
insert into REGISTRO_EVENTOS_DESTINOS
values (DESTINO, CODIGO, LLAMADAS, DURACION, FECHA)
```

*Nota.* En la figura se encuentra el query de registro con los diferentes campos necesarios para los eventos de fraude Wangiri por destino. Fuente: Propia.

Los querys de inserción de eventos deben ser ejecutados cada que se produzca un registro de tráfico atípico con tipología de fraude tanto individual por abonado como por destino. Se implementó un procedimiento en el programa de Back end encargada de generar este registro inmediatamente suceda el evento.

**Figura 24**

*Procedimiento de inserción de eventos*

```
Private Sub Actualizar_Tabla(codigo As String, llamadas As String, duracion As String, pais As String)
    Dim cnn_Actualizar_base As New OracleConnection
    cnn_Actualizar_base.ConnectionString = ("SERVER;USUARIO;PASSWORD;")
    Dim _SelectTable As String = ""
    Dim datos_base1 As New DataTable()
    Using cmd_Actualizar_base As New OracleCommand(_SelectTable, cnn_Actualizar_base)
        Using da As New OracleDataAdapter(cmd_Actualizar_base)
            Try

                Dim lineas(datos_base1.Rows.Count) As String
                Dim ingresar As String = "QUERY INSERCIÓN DE EVENTOS EN TABLA"
                cmd_Actualizar_base.CommandText = ingresar
                cmd_Actualizar_base.Connection.Open()
                cmd_Actualizar_base.ExecuteNonQuery()
                cmd_Actualizar_base.Connection.Close()
            Catch ex As Exception

            End Try

        End Using
    End Using
End Sub
```

*Nota.* En la figura se encuentra el procedimiento que se ejecuta para registrar un evento en la tabla creada respectivamente. Fuente: Propia.

El procedimiento Actualizar_Tabla es llamado dependiendo de la casuística de fraude que se esté tratando para almacenar la información en cada base de forma distintiva. El uso del método implementado en SqlCommand, ExecuteNonQuery, permite ejecutar sentencias del Lenguaje de Manipulación de Datos (DML) con el comando *insert* y devuelve el número total de filas afectadas en la ejecución de esta (ExecuteNonQuery, 2021).

**Notificaciones asertivas**

Al tratarse de un proceso de hilo infinito recurrente que se encuentra realizando la detección de posibles destinos y líneas fraudulentas, la cantidad de almacenamiento y notificación aumentaría si no se toman medidas de mitigación de alertas duplicadas.

Para el control de alertas se implementa un sistema comparativo en base a la referencia de alertas ocurridas durante la última revisión del incidente.

El control de destinos requiere de la extracción autónoma de un query de consulta de Oracle como el que se muestra en la Figura 24, el que extrae si un código de área fue detectado durante las últimas 12 horas.

**Figura 25**

*Query para validación de destino*

```
select codigo from REGISTRO_EVENTOS_DESTINOS
where codigo in ("CODIGO")
and
TO_DATE(FECHA, 'dd-mm-yyyy hh24:mi:ss') > sysdate-0.5
```

*Nota.* En la figura se encuentra el query de consulta para validar destinos ya notificados. Fuente: Propia.

De igual forma, para el control por abonado se desarrolla el query de consulta en Oracle con la finalidad de extraer los últimos parámetros de los clientes registrados como se muestra en la figura 25.

**Figura 26**

*Query para validación de línea*

```
SELECT MSISDN,DESTINO,LLAMADAS,DURACION,
MAX(TO_DATE(FECHA, 'dd-mm-yyyy hh24:mi:ss'))
FROM REGISTRO_EVENTOS_LDI
WHERE MSISDN IN ('" + linea + "')
GROUP BY MSISDN,DESTINO,LLAMADAS,DURACION
ORDER BY 5 DESC
```

*Nota.* En la figura se encuentra el query de consulta para extraer información de líneas ya notificadas. Fuente: Propia.

Para el control automático de notificaciones se validan los parámetros registrados en la tabla, se plantean los siguientes escenarios posibles:

- El valor de los minutos y llamadas no aumentaron, en este escenario se plantea que el comportamiento sigue siendo el mismo que la última notificación, por lo tanto, no se envía el correo electrónico.

- El valor de los minutos y llamadas aumentaron, en este escenario se plantea que el comportamiento aumentó respecto a la última notificación, por lo tanto, se envía el correo electrónico.

- El valor de los minutos y llamadas disminuyeron, al extraer información de la base de datos en un periodo de tiempo, puede existir disminución de los parámetros respecto a la última notificación, por lo tanto, no se envía el correo electrónico.

**Figura 27**

*Escenarios de notificación asertivas*

```
If (CStr(row("LLAMADAS")) = llamadas And CStr(row("DURACION")) = duracion And CStr(row("DESTINO")) = pais) Then
    Return 1
    cmd_validar_base_Teldi.Connection.Close()
ElseIf (CStr(row("LLAMADAS")) < llamadas Or (CStr(row("DURACION")) < duracion) And CStr(row("DESTINO")) = pais) Then
    Return 0
    cmd_validar_base_Teldi.Connection.Close()
ElseIf (CStr(row("LLAMADAS")) > llamadas Or (CStr(row("DURACION")) > duracion) And CStr(row("DESTINO")) = pais) Then
    Return 1
    cmd_validar_base_Teldi.Connection.Close()
End If
```

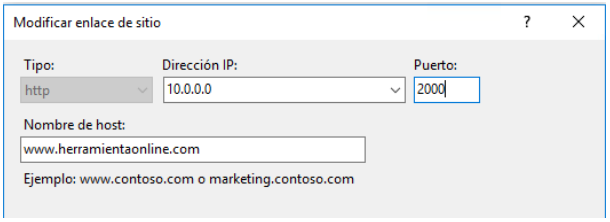
*Nota.* En la figura se encuentra el código para validar los tres escenarios planteados de notificaciones automáticas. Fuente: Propia.

**Configuración IIS**

Con la finalidad de que la herramienta pueda gestionar 24/7/365 es necesario cargar el web service generado en un servidor que tenga esa disponibilidad de funcionalidad y recursos, el programa se encuentra cargado en el servidor web de Microsoft IIS (que forma parte de la intranet de la empresa) con la siguiente configuración mostrada en la Figura 28.

**Figura 28**

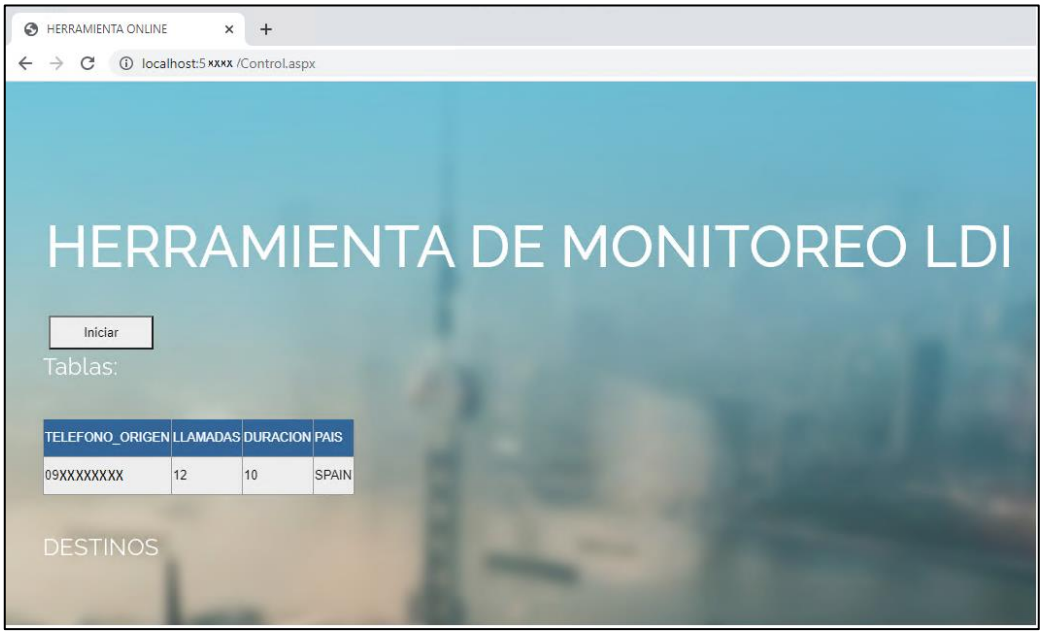
*Configuración Servidor IIS*




*Nota.* En la figura se encuentra el detalle de la configuración de la herramienta en el servidor web de Microsoft IIS. Fuente: Propia.

**Figura 29**

*Sistema online en funcionamiento*




*Nota.* En la figura se muestra la herramienta en el servidor web de Microsoft IIS. Fuente: Propia.

**Generación de Conocimiento**

Las fases de las metodologías desarrolladas desembocan en la generación del conocimiento para buscar soluciones que puedan ser útiles a las personas que están consumiendo la herramienta. Esta fase se encarga de poder compartir opciones a los usuarios con la finalidad de influir en la toma de decisiones. El sistema cuenta con dos aplicativos que proporcionan una mejor visión al usuario de los eventos de fraude, las mismas que son las notificaciones por correos electrónicos y la generación de tablas dinámicas en la herramienta de Business Intelligence PowerBI.

**Servicio de alertas vía correo electrónico**

Los eventos de fraude de llamadas de larga distancia internacional si no son tratados a tiempo pueden llegar a presentar un perjuicio económico tanto para la empresa como para el abonado, de igual forma, pueden llegar a representar un alto impacto mediático en el Ecuador. Por estos motivos, se requiere un sistema de notificación cercano al tiempo real que permita alertar de estos eventos para ser tratados de la forma óptima y oportuna posible.

El Namespace System.Net.mail permite utilizar clases orientadas al envío de correos electrónicos mediante el protocolo de simple transferencia de correos (SMTP) (System.Net.Mail, 2021). Se definen las clases que van a ser necesarias para satisfacer las necesidades de la herramienta diseñada.

Para el formato de correo enviado se recurre a la utilización de lenguaje HTML, se utiliza la constante vbCrLf que indica a texto que se está realizando un salto de línea.

**Figura 30**

*Procedimiento envío de correos Wangiri*

```
Public Sub Notificar_Evento_Destino(llamadas As String, duracion As String, pais As String, codigo As String)
    Dim message As New MailMessage
    Dim smtp As New SmtpClient

    With message
        .From = New System.Net.Mail.MailAddress("CORREO EMISOR")
        .To.Add("CORREO RECEPTOR")
        .Body = String.Format(String.Concat("Estimados,", vbCrLf, vbCrLf,
                                            "Se detecto un incremento de tráfico en el pais ", pais,
                                            " (código de área: ", codigo, ")",
                                            " con posible comportamiento WANGIRI: ", vbCrLf, vbCrLf,
                                            "Cantidad de llamadas: ", llamadas, vbCrLf,
                                            "Duración de llamadas: ", duracion, vbCrLf, vbCrLf,
                                            "Analizar el comportamiento del destino.", vbCrLf, vbCrLf,
                                            "Saludos.", vbCrLf))

        .Subject = "URGENTE: Alerta de Fraude WANGIRI REVISIÓN: " + pais
        .Priority = System.Net.Mail.MailPriority.High
    End With

    With smtp
        .EnableSsl = True
        .Port = "PUERTO"
        .Host = "SMTP HOST"
        .Credentials = New Net.NetworkCredential("CORREO", "PASSWORD")
        .Send(message)
    End With
    Try
        Response.Write("enviado")
    Catch ex As Exception
        Response.Write("error")
    End Try
End Sub
```

*Nota.* En la figura se encuentra el procedimiento que envía correos electrónicos de los destinos con posible fraude Wangiri. Fuente: Propia.

**Figura 31**

*Procedimiento envío de correos LDI*

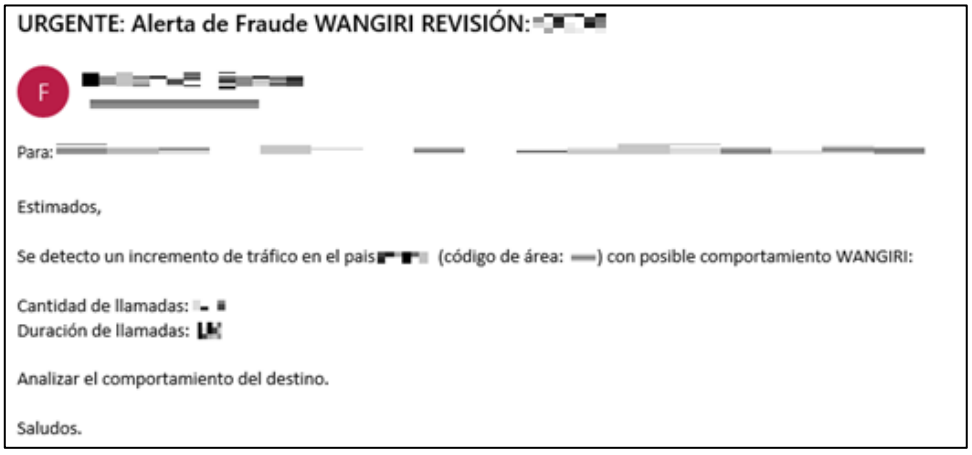
```
Public Sub Notificar_Evento_LDI(linea As String, llamadas As String, duracion As String, pais As String)
    Dim message As New MailMessage
    Dim smtp As New SmtpClient

    With message
        .From = New System.Net.Mail.MailAddress("CORREO EMISOR")
        .To.Add("CORREO RECEPTOR")
        .Body = String.Format(String.Concat(String.Concat("Estimados,", vbCrLf, vbCrLf,
                                                          "La línea ", linea,
                                                          " se encuentra realizando llamadas al destino ", pais,
                                                          " con el siguiente comportamiento:", vbCrLf, vbCrLf,
                                                          "Cantidad de llamadas: ", llamadas, vbCrLf,
                                                          "Duración de llamadas: ", duracion, vbCrLf, vbCrLf,
                                                          "Analizar el comportamiento de la línea.", vbCrLf, vbCrLf,
                                                          "Saludos.", vbCrLf)))

        .Subject = "URGENTE: Alerta de Fraude WANGIRI REVISIÓN: " + pais
        .Priority = System.Net.Mail.MailPriority.High
    End With
    With smtp
        .EnableSsl = True
        .Port = "PUERTO"
        .Host = "SMTP HOST"
        .Credentials = New Net.NetworkCredential("CORREO", "PASSWORD")
        .Send(message)
    End With
    Try
        Response.Write("enviado")
    Catch ex As Exception
        Response.Write("error")
    End Try
End Sub
```

*Nota.* En la figura se encuentra el procedimiento que envía correos electrónicos de las líneas con posible fraude LDI. Fuente: Propia.

El cuerpo del correo electrónico presenta un resumen de la información característica del evento suscitado, con la finalidad de que se pueda brindar una apreciación más rápida del incidente y sea mitigado ágilmente. A continuación, en la figura 32 y 33 se muestra un correo ejemplo de cada uno de los casos de fraudes generados anteriormente.

**Figura 32**

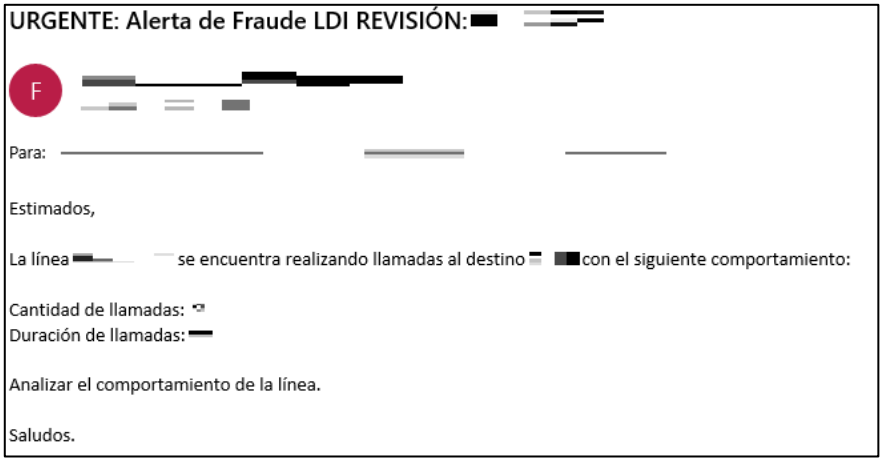
*Correo de notificación ejemplo Wangiri*




*Nota.* La figura muestra un correo ejemplo de notificación generado por la herramienta de un fraude Wangiri. Fuente: Propia.

**Figura 33**

*Correo de notificación ejemplo LDI*




*Nota.* La figura muestra un correo ejemplo de notificación generado por la herramienta de fraude Wangiri. Fuente: Propia.

**Tablero de indicadores front-end**

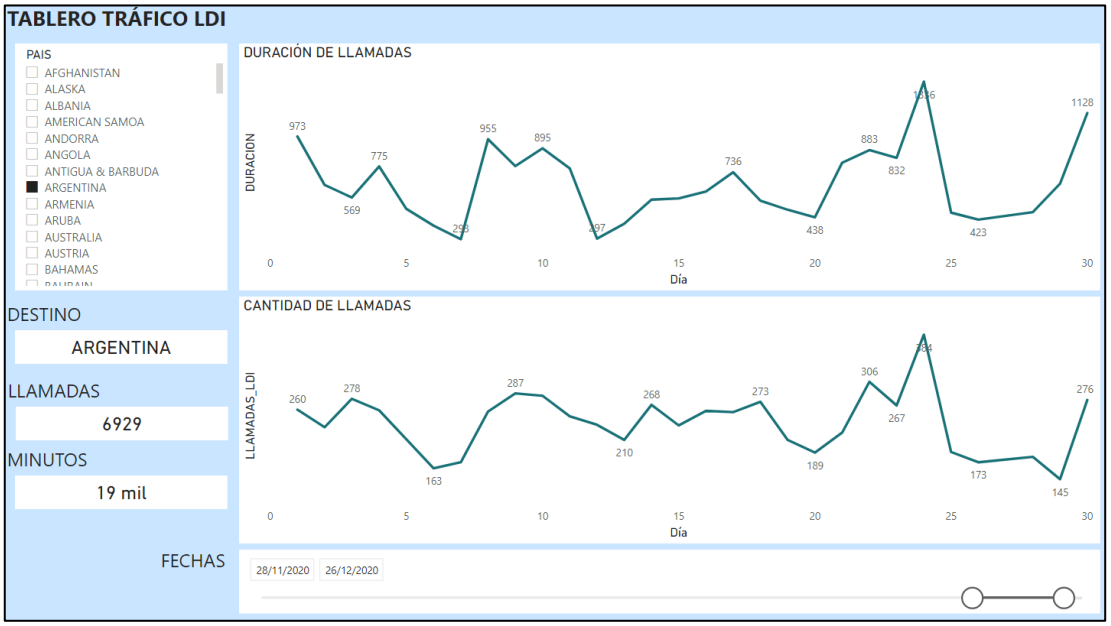
Con la finalidad de ofrecer un sistema de consulta de gráficas dinámicas en tiempo real, se diseña un tablero en la herramienta de Business Intelligence PowerBI, el mismo que cuenta con las siguientes características disponibles:

- Tendencias de cantidad de llamadas LDI por destino
- Tendencias de duración de llamadas LDI por destino
- Mapa de calor de minutos por destino
- Cantidad de líneas detectadas
- Cantidad de destinos detectados
- Filtros dinámicos

El tablero se encuentra publicado en el perfil empresarial y es compartido a todos los integrantes del área. El diseño de este es el mostrado en la Figura 34.

**Figura 34**

*Tablero de tendencias de tráfico LDI*

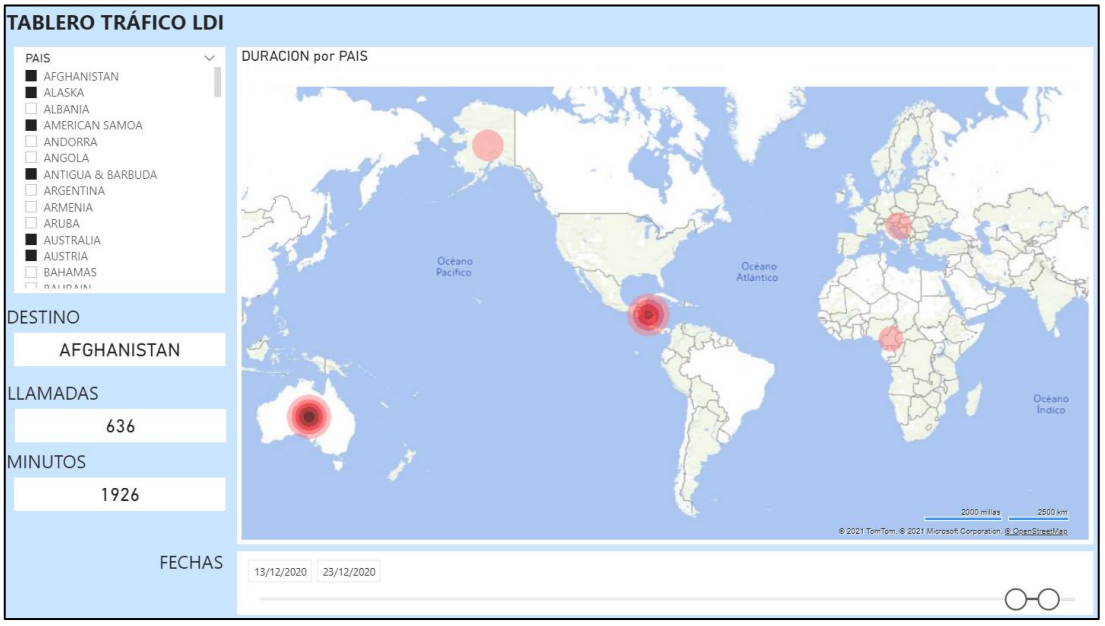



*Nota.* La figura muestra el tablero generado para el seguimiento de tendencias de fraudes LDI y Wangiri. Fuente: Propia.

PowerBI ofrece una gran variedad de objetos visuales para representar gráficamente los datos, desde la appsource propia de la herramienta, se importa el generador de mapas de calor Heat Map. El tablero para la visualización de este objeto es el mostrado en la figura 35.

**Figura 35**

*Mapa de calor de tráfico LDI*




*Nota.* La figura muestra el tablero generado para el seguimiento del mapa de calor del tráfico LDI. Fuente: Propia.

**Evaluación**

Para la evaluación de la herramienta, se diseñó un sistema de encuestas anónimas a todos los expertos del área de prevención de fraude de la empresa, la intención de la encuesta es corroborar en qué forma fue efectiva la detección y notificación de eventos de fraude durante el tiempo de funcionamiento de la herramienta.

Como segundo punto de evaluación es importante analizar los casos de éxito de detección de la herramienta para las diferentes casuísticas de fraude y qué impacto generan en la empresa. Todos estos análisis se encuentran documentados de forma teórica y gráfica en el apartado del capítulo de resultados.

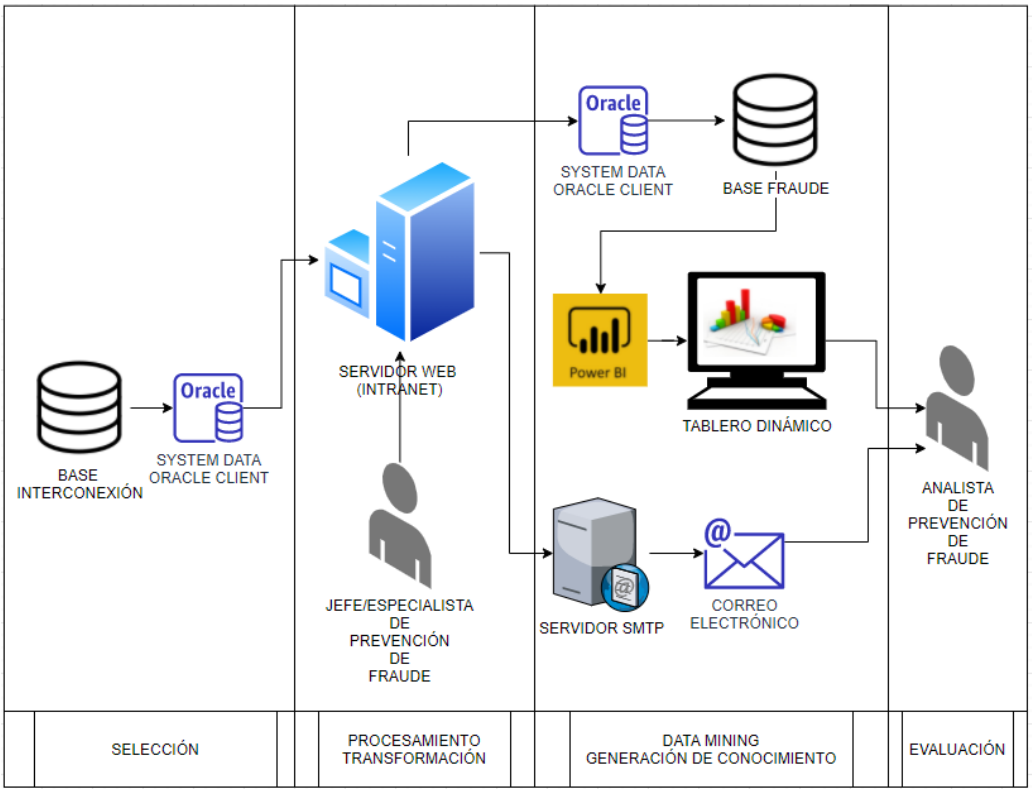
Después de concluir con todos los pasos de la metodología planteada, se logró un aplicativo que consta de fases de extracción de datos y fases de presentación de datos.

**Resultado Final**

Con la implementación de las metodologías planteadas y la puesta en producción de la herramienta desarrollada, se tiene en funcionamiento un aplicativo con la arquitectura mostrada en la Figura 36.

**Figura 36**

*Arquitectura del aplicativo*




*Nota.* La figura muestra la arquitectura del aplicativo desarrollado. Fuente: Propia.

## Validación de Resultados

### Informe de Resultados

Para el análisis de resultados se presentan los casos de éxito de detección después de la puesta en producción de la herramienta.

### Fraude Wangiri

### Fraude Wangiri Multidestino

El 26 de junio de 2020 se presentó un incidente a nivel país de tráfico atípico con tipología de fraude Wangiri de varios destinos, dicho incidente consistió en un bombardeo de llamadas desde múltiples destinos, esto ocasionó un creciente tráfico LDI de los abonados de la empresa hacia destinos de alto costo. El incidente presentó los siguientes problemas a ser considerados:

- Pérdidas económicas para la operadora
- Pérdidas económicas para los abonados
- Alto impacto mediático en el Ecuador (El Comercio, 2020)

Entre los destinos que más causaron revuelo en ese incidente se encuentran:

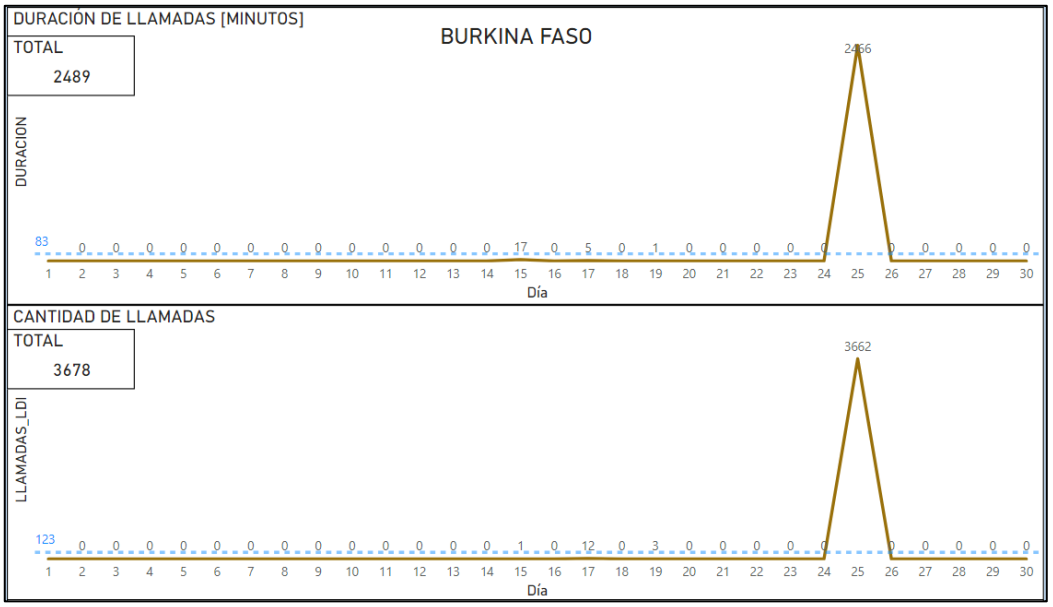
- Austria
- Burkina Faso
- Equatorial Guinea
- Georgia
- Liberia
- Mauritania
- Russia
- Serbia
- Surinam
- Tayikistán
- Turkey
- Turkmenistán

- Belarus
- Islas Vírgenes
- Zambia
- Marruecos
- Yugoslavia
- Latvia
- Nicaragua
- Uganda

La herramienta de fraude notificó a tiempo las alertas basadas en las tendencias de tráfico y los mapas de calor de cada uno de los destinos que se muestran en la Figura 37.

**Figura 37**

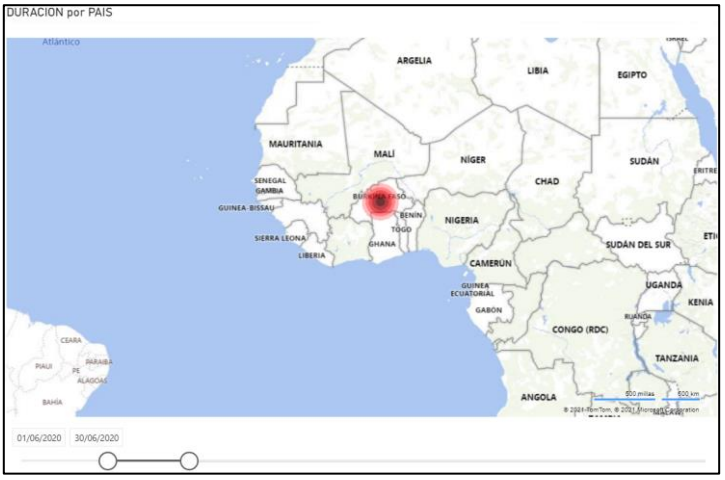
*Tendencia de tráfico Burkina Faso*




*Nota.* La figura muestra la tendencia de tráfico del destino Burkina Faso durante el incidente de fraude Wangiri del mes de junio del 2020. Fuente: Propia.

**Figura 38**

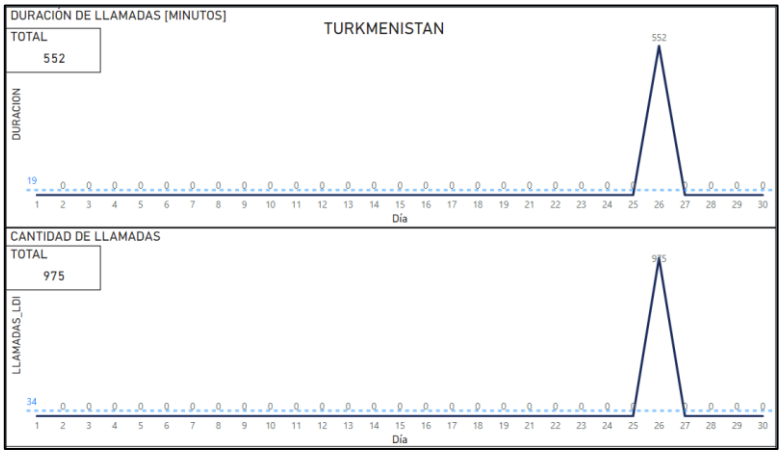
*Mapa de calor Burkina Faso*




*Nota.* La figura muestra el mapa de calor del destino Burkina Faso durante el incidente de fraude Wangiri del mes de junio del 2020. Fuente: Propia.

**Figura 39**

*Tendencia de tráfico Turkmenistán*




*Nota.* La figura muestra la tendencia de tráfico del destino Turkmenistán durante el incidente de fraude Wangiri del mes de junio del 2020. Fuente: Propia.

**Figura 40**

*Mapa de calor Turkmenistán*

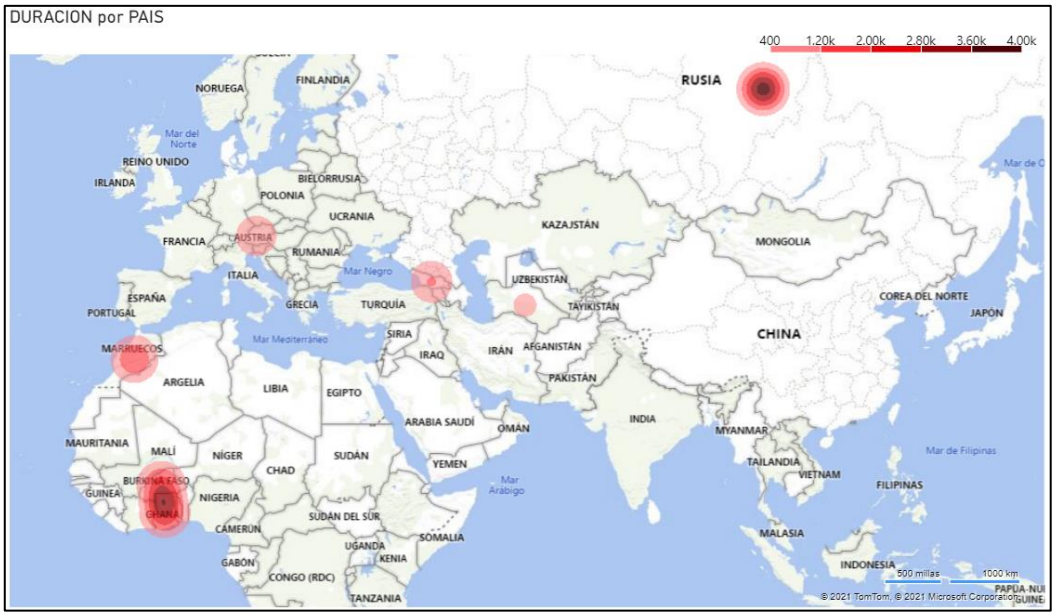

*Nota.* La figura muestra el mapa de calor del destino Turkmenistán durante el incidente de fraude Wangiri del mes de junio del 2020. Fuente: Propia.

Con la ayuda de las gráficas diseñadas y las notificaciones de alerta, se pudo obtener una mejor apreciación del conjunto de destinos que estaban realizando un ataque de bombardeo de llamadas hacia el Ecuador. Después de la pronta detección de la herramienta de monitoreo desarrollada y el análisis del equipo de prevención de fraude, se controló y mitigó el incidente. Evitando generar más perjuicios económicos a la empresa y a los abonados. Además, con la visibilidad global que ofrecían las gráficas dinámicas generadas, se detectaron nuevos destinos con las mismas tipologías de fraude, esto con la finalidad de generar una alerta en conjunto para reducir las pérdidas como país y calmar el álgido ambiente mediático que se estaba presentando

en redes sociales por la prensa y por los abonados.

**Figura 41**

*Fraude Wangiri Multidestino*



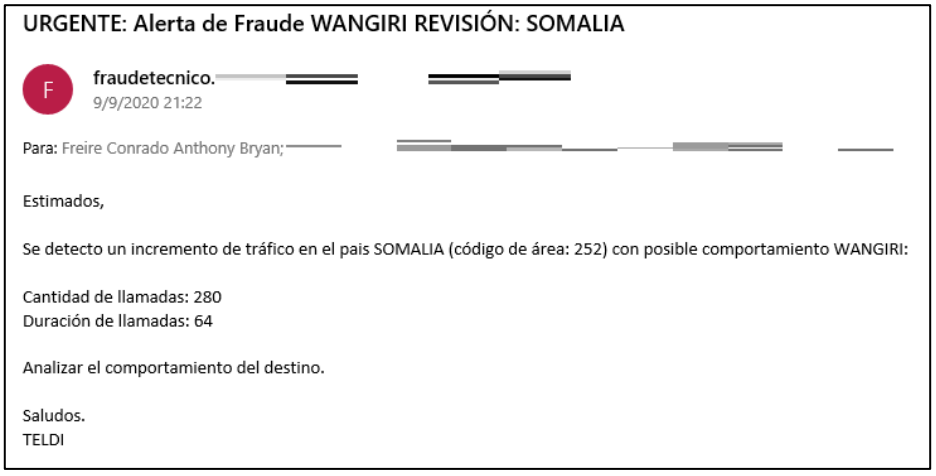

*Nota.* La figura muestra el mapa de calor de los destinos de alto riesgo durante el incidente de fraude Wangiri del mes de junio del 2020. Fuente: Propia.

**Fraude Wangiri Somalia**

En el mes de septiembre se presentó un comportamiento de tráfico atípico con tipología de fraude Wangiri hacia el destino de Somalia, como primer punto se presenta el correo de notificación alertando el evento que permitió al equipo realizar las acciones de mitigación pertinentes.

**Figura 42**

*Notificación de correo Wangiri Somalia*

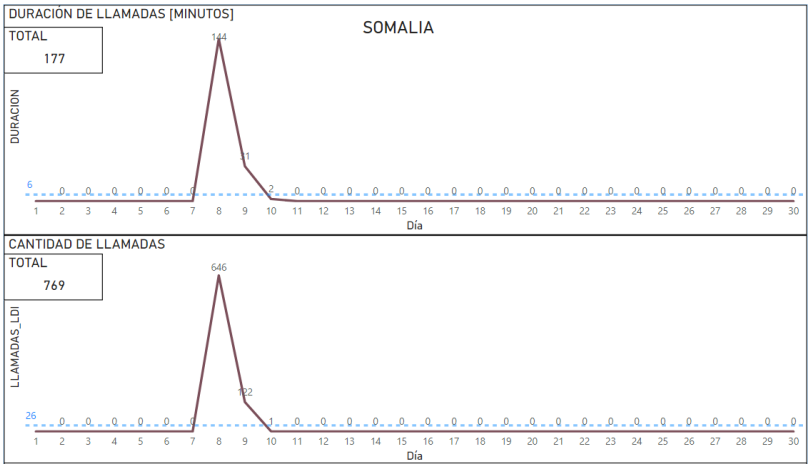



*Nota.* La figura muestra el correo electrónico de notificación ante el evento de fraude Wangiri hacia el destino Somalia. Fuente: Propia.

En la Figura 33 y 34 se presentan las gráficas de la tendencia de tráfico como el mapa de calor del destino que ayudaron a su detección y pronta mitigación.

**Figura 43**

*Tendencia de tráfico Wangiri Somalia*




*Nota.* La figura muestra la tendencia de tráfico del mes que ocurrió el evento de fraude Wangiri hacia el destino Somalia. Fuente: Propia.

**Figura 44**

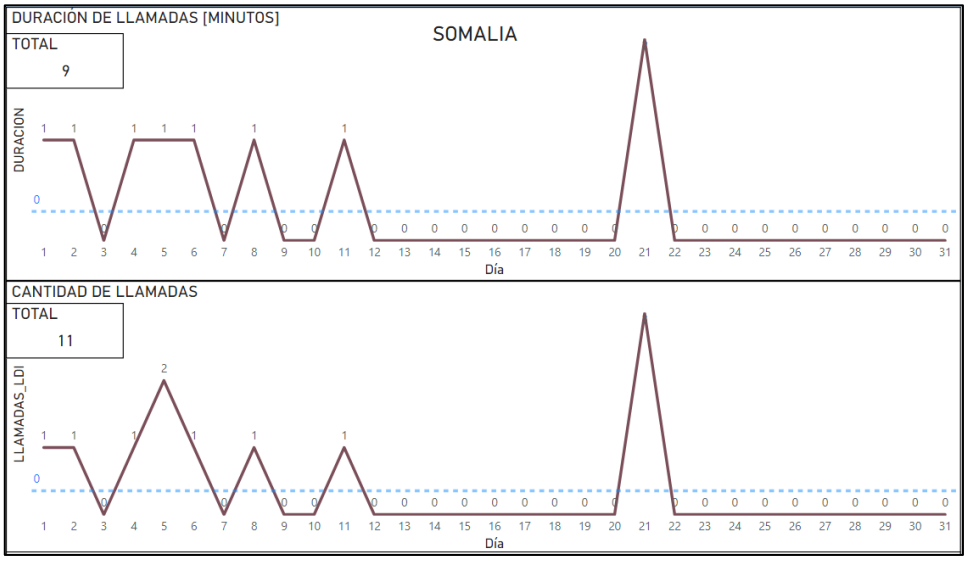
*Mapa de Calor Wangiri Somalia*


*Nota.* La figura muestra el mapa de calor del evento de fraude Wangiri hacia el destino Somalia. Fuente: Propia.

Se evidencia el incremento del tráfico tanto de llamadas como minutos hacia el destino que se está analizando, en comparativa con la Figura 45 que representa la tendencia de tráfico LDI en un mes en el que no ocurrieron incidentes de fraude. Se determinó un incremento de 769% del promedio de llamadas hacia el destino en un día, mostrando un claro comportamiento atípico con tipología de fraude Wangiri.

**Figura 45**

*Tendencia de tráfico a Somalia normal*




*Nota.* La figura muestra la tendencia de tráfico normal hacia el destino Somalia. Fuente: Propia.

**Fraude IRSF por hackeo PBX**

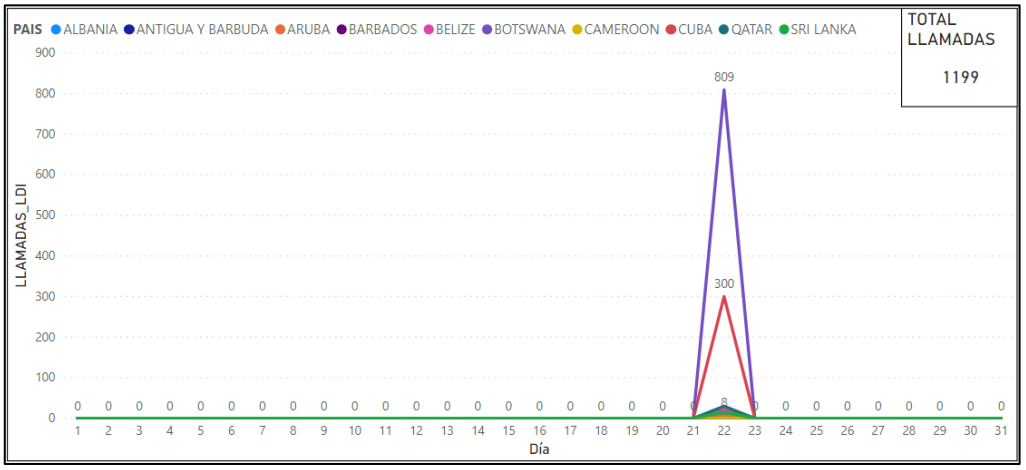
Las centrales telefónicas (PBX) cuentan con acceso a la navegación en internet, si dicho acceso no tiene los niveles de seguridad adecuados, los defraudadores buscan vulnerar y acceder a los sistemas con la finalidad de realizar llamadas hacia destinos de alto costo para generar pérdidas económicas a la empresa y obtener beneficios por las llamadas realizadas. Para la identificación del hackeo de una PBX, es importante basarse en las alarmas de notificación de

tráfico individual, para esto vamos a revisar el ejemplo de una empresa que sufrió una vulneración de seguridad hacia sus servidores.

En la figura 46 permite identificar la tendencia de tráfico que tuvo la central telefónica de la empresa hacia varios destinos de alto costo, esto debido a la intervención de un tercero en su sistema para realizar el bombardeo de llamadas.

**Figura 46**

*Tendencia de tráfico fraude PBX*




*Nota.* La figura muestra la tendencia de tráfico por hackeo a PBX. Fuente: Propia.

El incremento de tráfico hacia destinos que la empresa nunca había realizado ninguna llamada se puede evidenciar en la siguiente tabla:

**Tabla 9**

*Cantidad de llamadas por hackeo de PBX*

| LLAMADAS_LDI | PAÍS |
|---|---|
| 809 | BOTSWANA |
| 300 | CUBA |
| 22 | BELIZE |

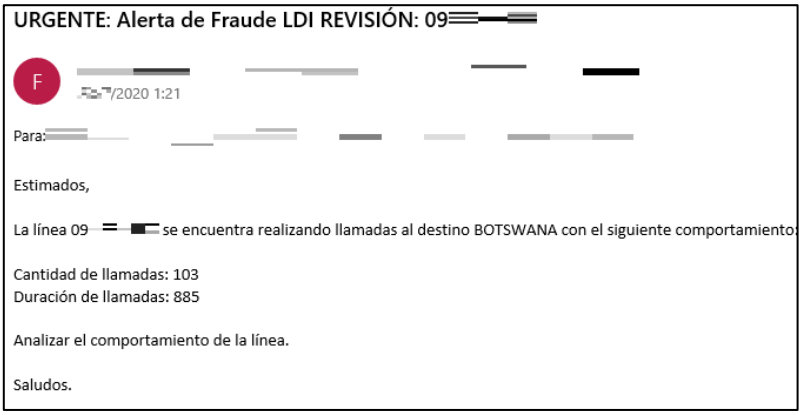
| | |
|---|---|
| 8 | ALBANIA |
| 30 | QATAR |
| 15 | SRI LANKA |
| 6 | ARUBA |
| 2 | CAMEROON |
| 2 | BARBADOS |
| 5 | ANTIGUA Y BARBUDA |

*Nota*. La tabla muestra la cantidad de llamadas por destino en el evento de hackeo a PBX. Fuente: Propia.

El primer registro que se generó en este incidente de fraude ocurrió a las 00:23am, la notificación vía correo electrónico, como se puede observar en la Figura 47, fue recibida a las 01:21 am. El periodo de tiempo, antes de que se tomaran acciones correctivas, fue de 58 minutos. Esto permite evidenciar la gran afectación que podría llegar a generarse si las alarmas no notifican a tiempo para tener una pronta mitigación. En base a esta pronta notificación y corrección, se pudieron evitar mayores pérdidas que se hubieran generado para la empresa, de esta manera, se asegura el bienestar del cliente.

**Figura 47**

*Notificación fraude LDI por hackeo de PBX*




*Nota.* La figura muestra el correo electrónico de notificación de fraude LDI por hackeo a PBX. Fuente: Propia.

**Fraude Roaming**

La herramienta de detección de fraude permite monitorear el comportamiento que tiene un abonado de otro país que se encuentra utilizando el servicio de Roaming internacional en el Ecuador, con la finalidad de notificar el consumo excesivo de llamadas que está generando un abonado visitante hacia diferentes destinos del mundo.

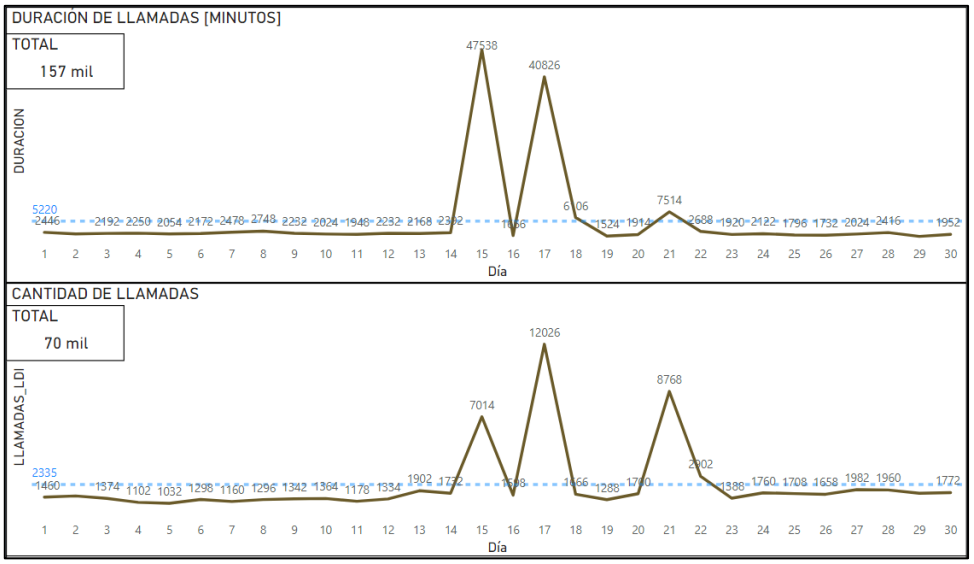
Se mantendrá de forma anónima el destino del cual eran originarios estos abonados, al destino al cual se realizaron las llamadas y la operadora a la que pertenecían con la finalidad de conservar la privacidad de los datos.

En el evento se registró en varios días del mes de junio de 2020, las llamadas realizadas desde la operadora de Ecuador hacia un destino de alto costo aumentaron fuera de las tendencias normales de tráfico como se muestra en la Figura 48. Los defraudadores realizan esto con la finalidad de generar costos de interconexión y de tal forma perjudicar tanto a la empresa origen

y visitante.

**Figura 48**

*Tendencia de tráfico por fraude de Roamers in*

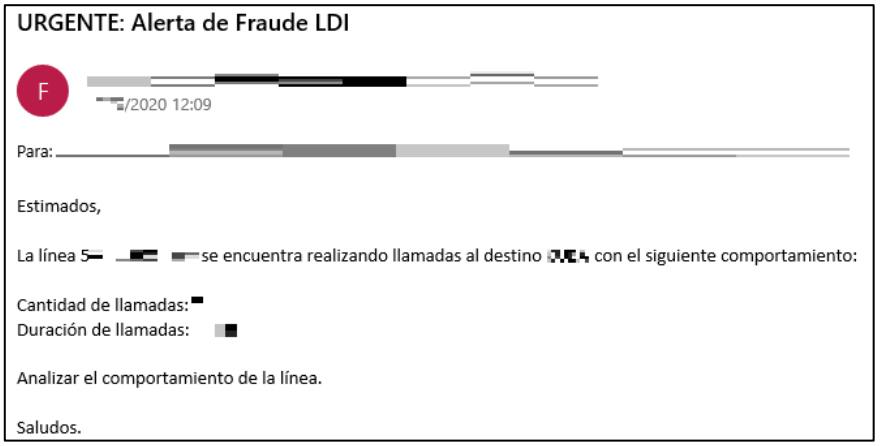



*Nota.* La figura muestra la tendencia de tráfico hacia el destino de alto costo realizado por Roamers in visitantes en la operadora de Ecuador. Fuente: Propia.

Es importante recalcar que el destino a pesar de ser considerado de alto costo presenta un tráfico relativamente alto. El total de líneas registradas como fraudulentas durante el evento fue de 29, se tuvieron todos los correos electrónicos con un promedio de notificación del evento de 1 hora y 54 minutos.

**Figura 49**

*Correo de notificación fraude Roaming*




*Nota.* La figura muestra el correo de notificación del incidente de fraude de Roaming. Fuente: Propia.

**Evaluación de comportamiento de la herramienta**

Para el análisis asertividad es necesario extraer todos los eventos que fueron detectados en cada una de las casuísticas controladas por la herramienta con la finalidad de determinar qué cantidad de falsos positivos existen. De igual forma, en la Figura 50 se presenta en formato de barras la comparativa en función de la casuística y su cantidad de casos detectados.

**Tabla 10**

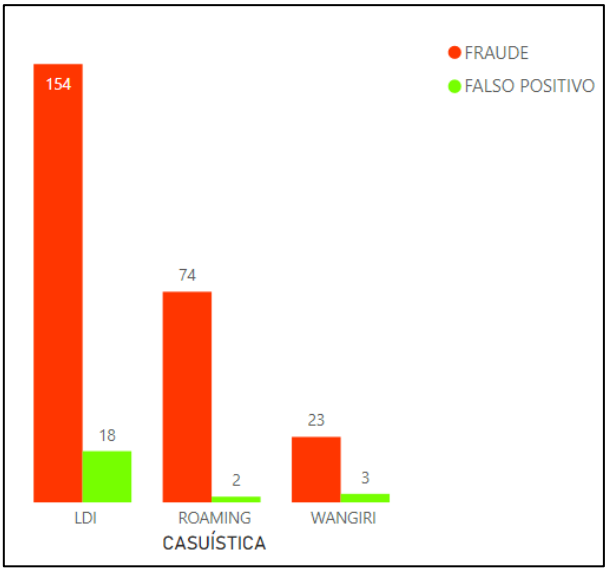
*Evaluación de Falsos Positivos*

| CASUÍSTICA | FRAUDE | FALSO POSITIVO | TOTAL |
|---|---|---|---|
| LDI | 154 | 18 | 172 |
| ROAMING | 74 | 2 | 76 |
| WANGIRI | 23 | 3 | 26 |

*Nota.* La tabla muestra la cantidad de casos efectivos en comparación con los falsos positivos en las diferentes casuísticas. Fuente: Propia.

**Figura 50**

*Comparativa de falsos positivos con fraudes por casuística*




*Nota.* La figura muestra la comparativa entre los casos de fraude detectados y los falsos positivos por casuística. Fuente: Propia.

El cálculo asertividad de una notificación enviada por la herramienta sea un evento de fraude está basado en cuantos eventos se tienen en total y cuantos eventos fueron casos confirmados con la formula mostrada en la Tabla 11.

**Tabla 11**

*Formula de la Asertividad*

$$\frac{\boldsymbol{CANTIDAD\ DE\ FRAUDES}}{\boldsymbol{TOTAL\ DE\ EVENTOS}} * \mathbf{100} \qquad \textbf{(1)}$$

*Nota.* La tabla muestra la formula usada para calcular asertividad de la herramienta desarrollada.

Fuente: Propia.

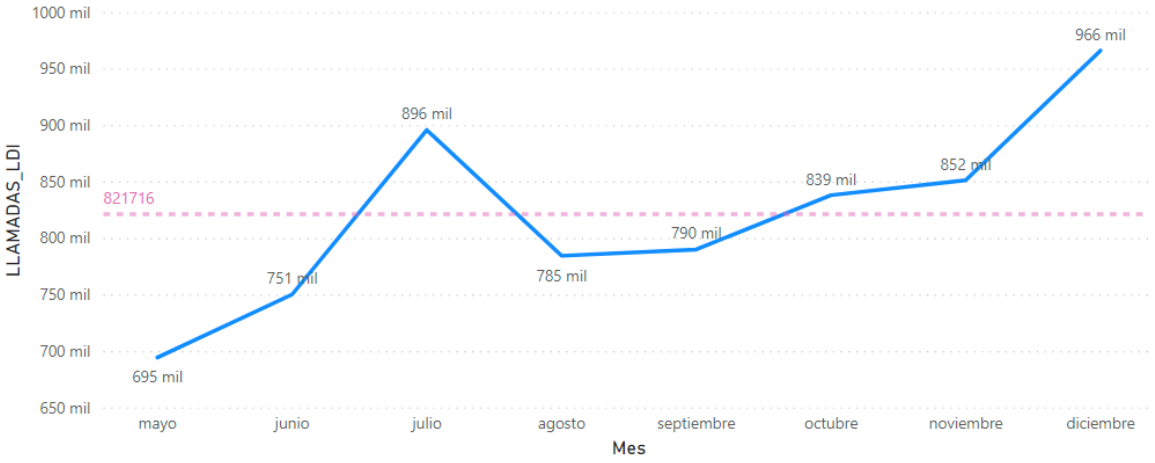
La aplicación desarrollada permite mitigar el 91.61% de las detecciones de fraude.

**Análisis del volumen de datos**

Con la finalidad de determinar la volumetría de datos que puede detectar el programa en diferentes intervalos de tiempo, se extrae la cantidad de llamadas de larga distancia internacional realizadas desde Ecuador hacia el resto del mundo, con esta información se determina el comportamiento de forma mensual como se muestra en la Figura 51.

**Figura 51**

*Tendencia de tráfico LDI mensual*

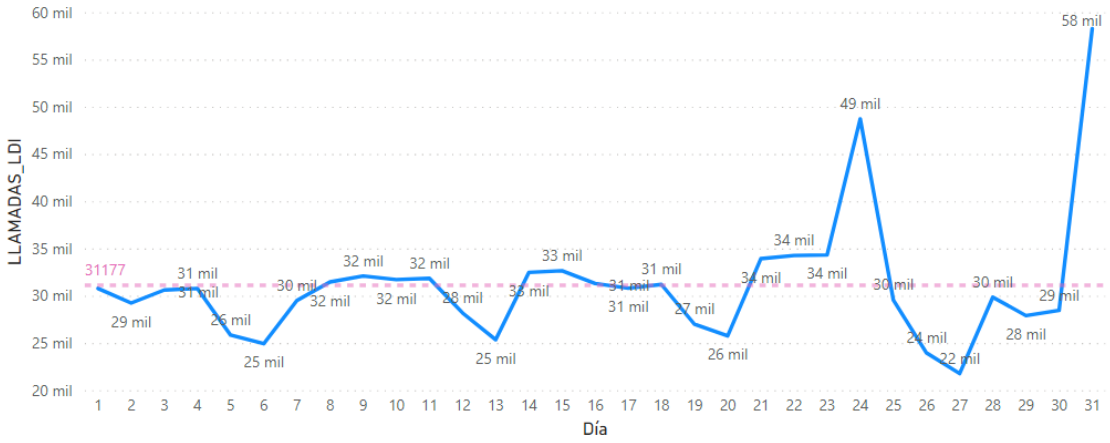



*Nota.* La figura muestra la tendencia mensual de las llamadas LDI. Fuente: Propia.

Como se observa en la Figura 51 se extraen grandes volúmenes de datos de forma mensual, teniendo como promedio 839.843 llamadas en un mes. Además, es importante recalcar que el promedio de llamadas de larga distancia internacional diarias es de 31.177 llamadas como se observa en la Figura 52.

**Figura 52**

*Tendencia de tráfico LDI diario*




*Nota.* La figura muestra la tendencia diaria de las llamadas LDI. Fuente: Propia.

**Análisis de la herramienta por expertos**

Con la finalidad de evaluar la herramienta por expertos, se creó un formulario en Google forms, el mismo fue realizado a los integrantes del equipo de prevención de fraude de la empresa con la finalidad de obtener una apreciación desde el punto de vista técnico y operativo de la herramienta. Cabe recalcar que la herramienta fue utilizada por todo el equipo y cada persona tiene conocimiento del funcionamiento y manejo de esta, esto con el objetivo de tener una respuesta objetiva y poder evaluar el nivel de satisfacción del área.

**Figura 53**

*Formulario creado en Google forms*


*Nota.* La figura muestra el formulario dispuesto para obtener la retroalimentación por parte de los expertos en análisis de fraudes. Fuente: Propia.

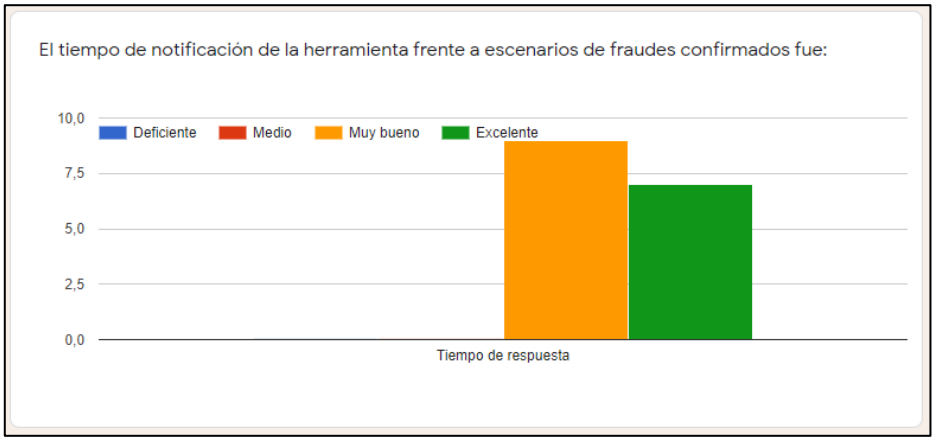
En base a tener un juicio de todas las personas que realizaron esta encuesta, se consideran los siguientes cargos a nivel empresa:

- Jefe de prevención de Fraude
- Especialista de prevención de Fraude
- Analista Sr de prevención de Fraude
- Analista de Prevención de Fraude

Como primer análisis es importante para estos casos entender que tan eficaz fue la herramienta al momento de notificar un evento de fraude, en base a las encuestas planteadas, podemos determinar que la herramienta tiene una calificación promedio de Muy buena a Excelente como se muestra en la Figura 54.

**Figura 54**

*Resultado de la encuesta a la pregunta 1*

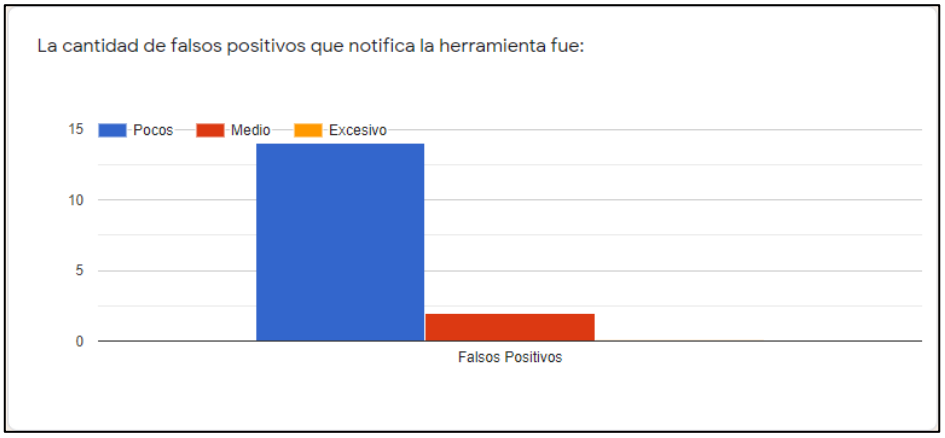



*Nota.* La figura muestra el gráfico generado en Google forms con las respuestas de los expertos a la pregunta 1. Fuente: Propia.

La finalidad de la herramienta es obtener la menor cantidad de falsos positivos al momento de notificar al equipo, esto orientado a que se necesita de mayor precisión para gestionar las alarmas, en base a las encuestas planteadas, podemos determinar que la herramienta tiene una calificación promedio de pocos falsos positivos como se muestra en la Figura 55.

**Figura 55**

*Resultado de la encuesta a la pregunta 2*

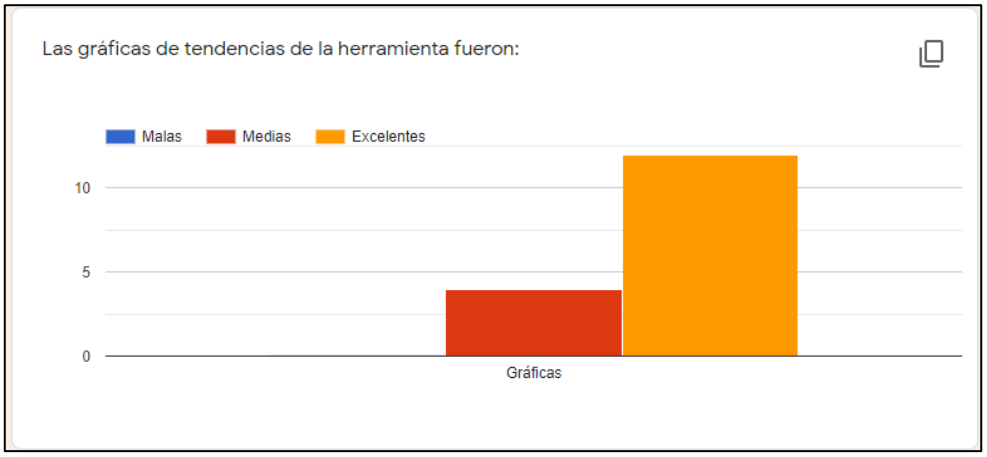



*Nota.* La figura muestra el gráfico generado en Google forms con las respuestas de los expertos a la pregunta 2. Fuente: Propia.

Las gráficas diseñadas con tendencias de tráfico y mapas de calor en Power BI ofrecen una mejor visibilidad de los posibles escenarios de fraude paralelos, en base a las encuestas planteadas, podemos determinar que la herramienta tiene una calificación promedio de que son excelentes al momento de la gestión como se muestra en la Figura 56.

**Figura 56**

*Resultado de la encuesta a la pregunta 3*

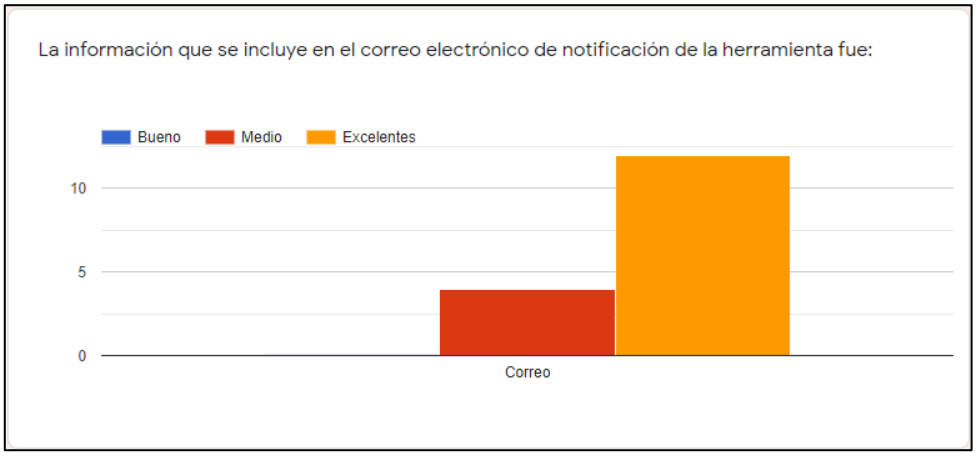



*Nota.* La figura muestra el gráfico generado en Google forms con las respuestas de los expertos a la pregunta 3. Fuente: Propia.

La información que se incluye en el correo electrónico de notificación es importante al momento de tomar decisiones en cortos tiempos, esto puede ayudar a dar más celeridad a las alertas emitidas, en base a las encuestas planteadas, podemos determinar que la información enviada por la herramienta es excelente como se muestra en la Figura 57.

**Figura 57**

*Resultado de la encuesta a la pregunta 4*




*Nota.* La figura muestra el gráfico generado en Google forms con las respuestas de los expertos a la pregunta 4. Fuente: Propia.

**Evaluación de tiempos de respuesta**

Los eventos de fraude en base a su criticidad pueden generar grandes pérdidas económicas a la empresa como a los abonados, las alertas de detección deben estar los más cercanas al tiempo real en el que está ocurriendo el incidente para que sea mitigado de forma óptima. Con la finalidad de evaluar la herramienta, se realizó un control de tiempos de respuesta de las notificaciones ante eventos de fraude. Estos eventos tuvieron los resultados mostrados en la Tabla 12.

**Tabla 12**

*Registro de tiempos de fraudes*

| N | INICIO DEL EVENTO (HORA) | REGISTRO BDD INTERCONEXIÓN (HORA) | NOTIFICACIÓN AUTOMÁTICA (HORA) | MITIGACIÓN DEL EVENTO (HORA) |
|---|---|---|---|---|
| Evento 1 | 17:54 | 18:09 | 19:14 | 19:29 |
| Evento 2 | 20:03 | 20:18 | 21:15 | 23:59 |
| Evento 3 | 18:19 | 18:34 | 19:18 | 20:03 |

*Nota.* La tabla muestra los tiempos de diferentes eventos de fraudes. Fuente: Propia.

Se calculó el periodo de tiempo entre el registro en la base de datos de Interconexión y la hora en la que llegó el correo electrónico con la notificación del incidente, el registro de esto se encuentra en la Tabla 13.

**Tabla 13**

*Tiempos de Notificación*

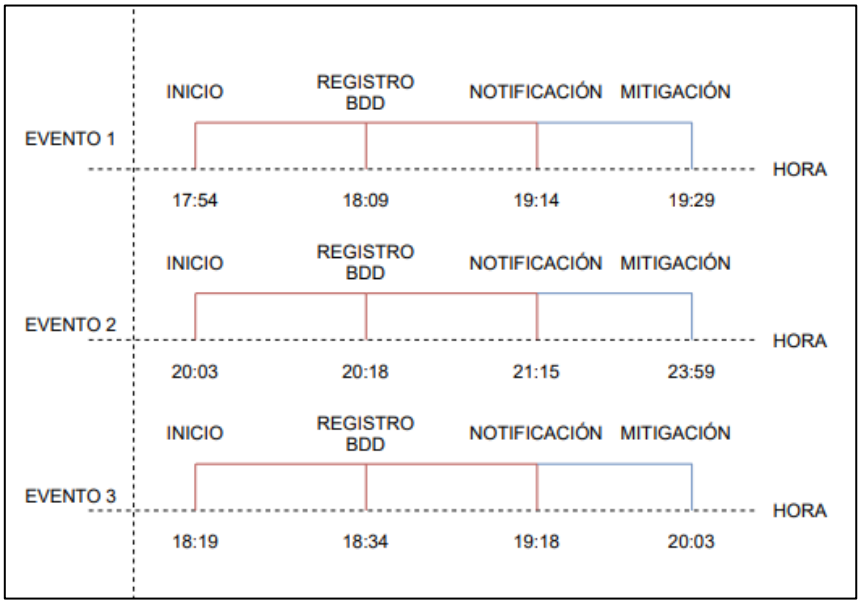
| N | REGISTRO BDD INTERCONEXIÓN (HORA) | NOTIFICACIÓN AUTOMÁTICA (HORA) | TIEMPO DE NOTIFICACIÓN |
|---|---|---|---|
| Evento 1 | 18:09 | 19:14 | 1:05 |
| Evento 2 | 20:18 | 21:15 | 0:57 |
| Evento 3 | 18:34 | 19:18 | 0:44 |

*Nota.* La tabla muestra los tiempos de diferentes eventos de fraudes. Fuente: Propia.

El tiempo promedio de notificación de la herramienta desarrollada es de 0:55 minutos, un valor bajo en cuanto al tratamiento de incidentes de fraudes en la empresa. Con este control implementado, se puede asegurar que la herramienta está notificando de forma óptima al equipo de prevención de fraude para que pueda actuar y mitigar el evento. Estos eventos transcurren en un periodo de tiempo desde que se produce el fraude hasta que es controlado por un experto en el tema como se muestra en la Figura 58.

**Figura 58**

*Diagrama de tiempo eventos de fraude*




*Nota.* La figura muestra un diagrama de tiempo con las horas en las que ocurrieron varios eventos de fraudes. Fuente: Propia.

**Resumen del Capítulo IV**

En este capítulo se expone los resultados que se obtienen después de la salida a producción de la herramienta desarrollada. En primer lugar, se formula una explicación teórica y práctica de cada una de las etapas de la metodología aplicada.

La definición del proyecto está orientada a considerar escenarios de fraudes basados en llamadas de larga distancia internacional, como primer objetivo es importante saber los registros de llamadas que se obtiene a nivel de la operadora. Para este punto en particular es necesario tener un know-how de la empresa que permita buscar la información necesaria en diferentes

áreas del negocio. Uno de los principales parámetros que se requiere de los datos obtenidos es que sean almacenados lo más cercano al tiempo real. Después de analizar de forma interna toda la información que se tiene en la empresa, se logró identificar una base de datos en la que se guardan estas llamadas con un tiempo de actualización bajo que cumple con los requerimientos de la herramienta.

Las bases de datos se encuentran en los servidores de la empresa, por lo que es fundamental entender qué información tenemos disponible y cómo extraerla. Al ser esta data manejada por otra parte del negocio, es necesario solicitar permisos de lectura hacia las tablas necesarias.

En la etapa de selección de datos se especifican qué campos vamos a mapear en los querys de consulta y mediante las funciones propias de Oracle se pueden realizar diferentes tipos de tablas acumuladas. Con estas tablas generadas, es necesario que el programa extraiga la información en un periodo de tiempo determinado.

El desarrollo generado en Visual Studio permite que se consulten los registros de forma autónoma, permanente y con disponibilidad 24/7/365 sin ninguna interacción humana. Con esto se logra reducir la carga operativa del control de fraude LDI.

Consecuentemente, después de que el sistema fue puesto en producción, se recibían las notificaciones de correo electrónico con la finalidad de poder tener una alerta temprana del evento para que pueda ser mitigado a tiempo y evitar generar incidencias económicas tanto a la empresa como a los abonados, dependiente de la casuística de fraude que se esté manejando.

La herramienta encontró varios patrones de fraude que de forma manual serían muy

complejos. Basándose en estos escenarios, se pudieron ir corrigiendo los umbrales con la finalidad de tener un control más estricto con la menor cantidad de falsos positivos posibles a lo largo del tiempo.

En base a la experiencia en control, los eventos de fraudes son variantes y pueden presentar tendencias de control con diferentes periodos de tiempos, la herramienta presenta un tiempo de notificación óptimo de 55 minutos que permiten mitigar el evento de forma más proactiva evitando que la masificación de llamadas siga en aumento.

El porcentaje de detección de casos de fraude de la herramienta según los análisis de los casos notificados es del 91.61%, esto indica que el revisar las alarmas enviadas pueden evitar en su totalidad los casos de fraudes ocurridos en llamadas de larga distancia internacional. Podemos afirmar que se van a controlar en un 100% los casos de fraude que notifique la herramienta, esto debido a que todas las alarmas enviadas son revisadas por personas expertas en el tema y los casos de fraudes positivos serán descartados y no tendrán incidencia ni en la empresa ni en el cliente.

# Conclusiones y Recomendaciones

## Conclusiones

Con el estudio del arte se incrementó el conocimiento respecto a las diferentes casuísticas de fraude a nivel internacional y las técnicas que se utilizan para la mitigación de estas por parte de otras operadoras mundiales. En base a los artículos obtenidos mediante el Systematic Mapping Studies y la experiencia obtenida en el manejo de fraudes de llamadas de larga distancia internacional, se logra tener una visión más amplia que permite desarrollar patrones de detección óptimos.

El uso en conjunto de las metodologías KDD y CRISP-DM permitió obtener un modelo sistemático que facilitó cada una de las etapas de desarrollo de la herramienta. Los procesos de selección, procesamiento y transformación permiten encaminar al objetivo del diseño. El proceso de Data Mining permite generar patrones para lograr resultados. La generación de conocimiento y evaluación permiten tomar decisiones frente a eventos de fraude ocurridos y mejoras a la herramienta.

Basándose en las metodologías implementadas para el proyecto, se desarrolla la herramienta de monitoreo cercano al tiempo real de tráfico de larga distancia internacional. Desde que la automatización fue puesta en producción se tuvieron las notificaciones por correo electrónico, estás alarmas facilitaron la detección temprana de posibles fraudes a lo largo del tiempo, el programa presenta asertividad del 91.61% en sus alertas por lo que se tiene que exige un control riguroso de las mismas.

Las herramientas de Business Intelligence como Power BI permiten tener una apreciación

más dinámica y gerencial de los incidentes de fraude, por medio de las gráficas de control implementadas se puede tener un campo de visión mundial que permite detectar nuevos eventos de fraudes que se encuentran ocurriendo de forma paralela. Además, permiten tener de forma visual todos los controles que está realizando la herramienta.

El sistema ha funcionado sin ningún inconveniente a lo largo de su control con el tiempo, no se han presentado incidentes de caídas del servicio de notificación lo cual nos da la confianza de que el monitoreo de fraudes se encuentra respaldado y automatizado.

El servicio de notificaciones automáticas de fraudes tiene un costo planteado por un proveedor externo, en el caso de la herramienta que tenía antes la empresa el valor que se pagaba al año era de $260.000 dólares. El tener un desarrollo in-house presenta un gran ahorro para la empresa y ese dinero puede ser destinado a diferentes áreas del negocio que ayudan a mantener un excelente servicio de calidad y precio hacia los clientes.

Basándose en encuestas realizadas a expertos que conforman el área de prevención de fraude, se tiene un 100% de calificaciones excelentes y muy buenas respecto al tiempo de notificación de la herramienta y un 87.5% de opiniones que la herramienta notifica pocos falsos positivos. Los resultados demuestran que existe satisfacción en las notificaciones, en los tiempos de respuesta, notificación de falsos positivos e información frente a un evento de fraude.

**Recomendaciones**

Las metodologías de inteligencia de negocios permiten seguir un proceso sistematizado y ordenado con la finalidad de lograr un objetivo específico. La implementación de estas logrará obtener mejores resultados en tiempos de desarrollo, producción y pruebas de forma óptima.

El uso de herramientas de visualización de Inteligencia de Negocios como PowerBI o Tableau permiten obtener gráficas que pueden ser presentadas de una forma más sobria y gerencial con la finalidad de presentar datos de forma dinámica y entendible al público.

Con la finalidad de que se pueda tener un control óptimo y una pronta mitigación de un evento de fraude, es necesaria la implementación de herramientas lo más cercanas posibles al tiempo real.

Se recomienda implementar el servidor de correos electrónicos para las notificaciones directamente de Exchange de la empresa con la finalidad de conservar los datos por el tipo de información que se maneja.

**Bibliografía**

Camacho Sellán, K. M., & González Mora, M. G. (2016). Diseño de un Sistema de Detección y Control del Fraude en la Prestación de los Servicios de Telefonía Fija y Servicio Móvil Avanzado en el Ecuador. Facultad de Ingeniería en Electricidad y Computación. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, 40-43.

Constantinos, H. (2010). Designing an expert system for fraud detection in private telecommunications networks. Expert Systems with ApplicationsVolume 36, Issue 9, 11559-11569. https://doi.org/10.1016/j.eswa.2009.03.031.

DataGridView. (2021). Microsoft DataGridView Class Documentation. Obtenido de https://docs.microsoft.com/en-us/dotnet/api/system.windows.forms.datagridview?view=net-5.0

El Comercio. (27 de 06 de 2020). El Comercio, ¿Extrañas llamadas internacionales en su celular? Recomendaciones. Obtenido de https://www.elcomercio.com/actualidad/llamadas-burkina-faso-policia-ecuador.html

ExecuteNonQuery. (2021). SqlCommand.ExecuteNonQuery Method Microsoft Documentation. Obtenido de https://docs.microsoft.com/en-us/dotnet/api/system.data.sqlclient.sqlcommand.executenonquery?view=dotnet-plat-ext-5.0

Gabriel, F. (2008). El fraude en roaming: estrategias de ataque y defensa. Taller IIRSA / CITEL "Servicios de roaming internacional" Universidad de Granada (España).

Humberto, R., & Bermudez, C. (05 de Febrero de 2019). Análisis del proyecto de software: “control anti-fraude roaming internacional in”. Obtenido de

http://repositorio.unimagdalena.edu.co/jspui/bitstream/123456789/4383/1/IS-00214.pdf

INEC. (2018). Tecnologías de la Información y Comunicación. Obtenido de Encuesta Multipropósito - TIC 2018: ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2018/201812_Principales_resultados_TIC_Multiproposito.pdf

López Dávila, J. (2018). Análisis y Visualización de los datos reportados de telefonía móvil a la ARCOTEL. Escuela Superior de Ingeniería y Tecnología Universidad Internacional de La Rioja (UNIR).

Mais, A., Abdallah, Q., & George, S. (2019). Detection of Wangiri Telecommunication Fraud Using Ensemble Learning. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 10.1109/JEEIT.2019.8717528.

Olszewski, D. (2012). A probabilistic approach to fraud detection in telecommunications. Knowledge-Based Systems Volume 26, 246-258. https://doi.org/10.1016/j.knosys.2011.08.018.

Saharon, R., Uzi, M., Einat, N., Yizhak , I., & Gadi , P. (2012). Discovery of Fraud Rules for Telecommunications - Challenges and Solutions. Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining, 409–413 https://doi.org/10.1145/312129.312303.

Shing-Han, L., Yen, D. C., Wen-Hui, L., & Chiang, W. (2012). Identifying the signs of fraudulent accounts using data mining techniques. Computers in Human Behavior Volume 28, Issue 3, 1002-1013. https://doi.org/10.1016/j.chb.2012.01.002.

System.Net.Mail. (2021). System.Net.Mail Namespace Microsoft Documentation. Obtenido de https://docs.microsoft.com/en-us/dotnet/api/system.net.mail?view=net-5.0

Timer. (2021). Microsoft Timer Class Documentation. Obtenido de https://docs.microsoft.com/en-us/dotnet/api/system.web.ui.timer?view=netframework-4.8