



UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA:

**IMPLEMENTACIÓN “THE FRAUD EXPLORER FTA” EN LA
EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE
PREVENCIÓN Y DETECCIÓN DE FRAUDE**

AUTOR:

RONALD FERNANDO COLOMA ANDAGOYA

TUTOR:

ING. CHRISTIAN PATRICIO BENALCAZAR VACA CPA MSC.

QUITO, ECUADOR

2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: “IMPLEMENTACIÓN THE FRAUD EXPLORER FTA EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE”, ha sido desarrollado por el señor Ronald Fernando Coloma Andagoya con C.C. No. 1722201827 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

Ronald Fernando Coloma Andagoya

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación “**IMPLEMENTACIÓN THE FRAUD EXPLORER FTA EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE**”, presentado por Ronald Fernando Coloma Andagoya, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M., 15 de febrero de 2019

TUTOR

Ing. Christian Patricio Vaca Benalcazar CPA Msc.

AGRADECIMIENTOS

Agradezco este trabajo a:

A dios y a mi madre que desde el cielo bendicen mi vida todos los días, gracias a ella por enseñarme que a lo largo de nuestra vida debemos disfrutarla a cada momento como si fuera el último.

A mi padre Hugo Ramos por ser un ejemplo de vida, esa muestra de lucha y superación constante, gracias por inculcar en mí que la responsabilidad, el esfuerzo y la valentía nos llevan a conseguir nuestras metas por más difíciles que parezcan.

A mi esposa Paulina y a mi hijo Martin que son mi razón de vivir y esforzarme cada día para ser un mejor esposo, padre y persona.

A mi tutor Ing. Christian Vaca CPA Msc. por brindar la oportunidad de trabajar de la mano y con su apoyo sacar adelante este proyecto.

A la Universidad Israel que conjuntamente con sus directivos y docentes nos forman para ser mejores profesionales cada día.

A mis compañeros y amigos en especial a Gustavo, Carlos y Jostin que juntos desde el inicio conformamos un excelente equipo de trabajo y supimos ayudarnos mutuamente.

DEDICATORIA

Dedico este trabajo a:

 Mi madre que, aunque ya no está con nosotros y sé que desde el cielo ella estará orgullosa por este logro alcanzado.

 Mi padre, esposa e hijo por su cariño y apoyo incondicional, por estar para mí siempre que los necesite gracias. A mi familia por todos sus consejos y palabras de aliento durante todo este proceso.

 Mi tutor Ing. Christian Vaca CPA Msc. por su guía y atención a mis consultas en toda la etapa de la elaboración del proyecto.

TABLA DE CONTENIDOS

RESUMEN	XI
ABSTRACT	XII
INTRODUCCIÓN	13
ANTECEDENTES DE LA SITUACIÓN OBJETO DE ESTUDIO	13
PLANTEAMIENTO DEL PROBLEMA	14
JUSTIFICACIÓN	14
OBJETIVOS.....	14
<i>OBJETIVO GENERAL.....</i>	<i>14</i>
<i>OBJETIVOS ESPECÍFICOS.....</i>	<i>15</i>
DESCRIPCIÓN DE LOS CAPÍTULOS.....	15
1 CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA	16
1.1 ESTADO DEL ARTE.....	16
1.1.1 <i>FRAUDE.....</i>	<i>17</i>
1.1.2 <i>TIPOS DE FRAUDE.....</i>	<i>18</i>
1.1.3 <i>MODELOS DE FRAUDE.....</i>	<i>21</i>
1.1.4 <i>TÉCNICAS DE FRAUDE UTILIZANDO EQUIPOS DE CÓMPUTO.....</i>	<i>23</i>
1.1.5 <i>SEGURIDAD DE LA INFORMACIÓN.....</i>	<i>25</i>
1.1.6 <i>RIESGO.....</i>	<i>26</i>
1.1.7 <i>REGULACIÓN LOCAL PARA DELITOS INFORMÁTICOS.....</i>	<i>28</i>
1.2 LÓGICA DEL NEGOCIO.....	29
1.2.1 <i>LINEAS DE NEGOCIO.....</i>	<i>30</i>
1.3 HERRAMIENTAS TÉCNICAS	31
1.3.1 <i>COMPONENTES DE LA SOLUCIÓN.....</i>	<i>31</i>
1.3.2 <i>CONCEPTUALIZACIÓN.....</i>	<i>32</i>
1.4 ALTERNATIVAS DE SOLUCIÓN.....	32
2 CAPÍTULO II. MARCO METODOLÓGICO	34
2.1 TIPO DE INVESTIGACIÓN.....	34
2.2 RECOPIACIÓN DE INFORMACIÓN	34
2.2.1 <i>TÉCNICAS DE RECOPIACIÓN DE INFORMACIÓN.....</i>	<i>34</i>
3 CAPÍTULO III. PROPUESTA	37
3.1 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL.....	37
3.1.1 <i>FACTIBILIDAD TÉCNICA.....</i>	<i>37</i>
3.1.2 <i>FACTIBILIDAD OPERACIONAL.....</i>	<i>38</i>

3.1.3	FACTIBILIDAD ECONÓMICA	39
3.1.4	MODELO O ESTÁNDAR A APLICAR.....	40
4	CAPÍTULO IV. IMPLEMENTACIÓN	44
4.1	APLICACIÓN DEL MODELO, ESTÁNDAR O METODOLOGÍA	44
4.1.1	DESARROLLAR EL ACTA DE CONSTITUCIÓN DEL PROYECTO.....	44
4.1.2	IDENTIFICAR A LOS INTERESADOS	44
4.1.3	PLANIFICAR LA GESTIÓN DEL ALCANCE	44
4.1.4	PLANIFICAR LA GESTIÓN DEL CRONOGRAMA	46
4.1.5	PLANIFICAR LA GESTIÓN DE LOS RIESGOS.....	49
4.1.6	PLANIFICAR LA GESTIÓN DE LOS RECURSOS.....	51
4.1.7	PLANIFICAR LA GESTIÓN DE LOS COSTOS.....	51
4.1.8	ESTIMAR LOS RECURSOS DE LAS ACTIVIDADES	51
4.1.9	ESTIMAR LA DURACIÓN DE LAS ACTIVIDADES.....	52
4.1.10	DETERMINAR EL PRESUPUESTO	52
4.1.11	PLANIFICAR LA GESTIÓN DE LA CALIDAD.....	53
4.1.12	PLANIFICAR LA GESTIÓN DE LAS COMUNICACIONES.....	53
4.1.13	PLANIFICAR LA GESTIÓN DE LAS ADQUISICIONES.....	54
4.1.14	DIRIGIR Y GESTIONAR EL TRABAJO DEL PROYECTO	54
4.1.15	GESTIONAR EL CONOCIMIENTO DEL PROYECTO	54
4.1.16	GESTIONAR LAS COMUNICACIONES	54
4.1.17	GESTIONAR LA CALIDAD	54
4.1.18	MONITOREAR Y CONTROLAR EL TRABAJO DEL PROYECTO	55
4.1.19	REALIZAR EL CONTROL INTEGRADO DE CAMBIOS.....	56
4.1.20	CONTROLAR EL CRONOGRAMA.....	56
4.1.21	MONITOREAR LAS COMUNICACIONES	56
4.1.22	MONITOREAR LOS RIESGOS.....	56
4.1.23	CONTROLAR LA CALIDAD	56
4.1.24	CONTROLAR LOS RECURSOS.....	57
4.1.25	VALIDAR Y CONTROLAR EL ALCANCE.....	57
4.1.26	CIERRE DEL PROYECTO.....	58
4.2	DISEÑO	58
4.2.1	DESCRIPCIÓN	58
4.2.2	IMPLEMENTACIÓN THE FRAUD EXPLORER.....	59
4.2.3	OPERACIÓN THE FRAUD EXPLORER.....	72
4.2.4	ADMINISTRACIÓN THE FRAUD EXPLORER.....	75
4.2.5	RESULTADOS.....	77
4.2.6	PRUEBAS REALIZADAS	80

5	CONCLUSIONES	82
6	RECOMENDACIONES	83
7	REFERENCIAS BIBLIOGRÁFICAS.....	84
8	ANEXOS.....	89

LISTA DE FIGURAS

Figura 1.1 Regla del 10 80 10	18
Figura 1.2 Elementos de la Corrupción.....	20
Figura 1.3 Diamante del Fraude	23
Figura 1.4 Mapeo Delitos COIP	28
Figura 1.5. Diagrama de flujo proceso de comercialización.....	30
Figura 2.6. Misión, visión y política de CELCO Cía. Ltda.....	37
Figura 3.7 Organigrama Departamento Sistemas CELCO Cía. Ltda.....	38
Figura 4.8 Gestión de la implementación.....	46
Figura 4.9 Secuencia de Actividades de la Gestión del Proyecto	49
Figura 4.10 Infraestructura de red CELCO Cía. Ltda.	58
Figura 4.11 Ubicación archivos fuente.....	60
Figura 4.12 Login The Fraud Explorer	72
Figura 4.13 Ventana principal	73
Figura 4.14 Ventana Endpoints	73
Figura 4.15 Ventana analytics	74
Figura 4.16 Detalle Analytics.....	74
Figura 4.17 Detalle alertas.....	75
Figura 4.18 Configuración reglas	75
Figura 4.19 Configuración principal	76
Figura 4.20 Administración de roles	76
Figura 4.21 Mantenimiento	77
Figura 4.22 Diagrama de proceso The Fraud Explorer	78
Figura 4.23 Resultados simulación 1	79
Figura 4.24 Resultados simulación 2	79

LISTA DE TABLAS

Tabla 1.1 Clasificación de percepción de corrupción	21
Tabla 1.2 Elementos del Fraude	22
Tabla 1.3 Tipos de información	26
Tabla 1.4 Código del Trabajo	29
Tabla 1.5 Catálogo de productos	30
Tabla 1.6 Componentes de The Fraud Explorer.....	31
Tabla 1.7 Conceptualización	31
Tabla 1.8 Soluciones Alternativas	32
Tabla 2.1 Resumen Casos de Fraude.....	36
Tabla 3.1 Requerimiento mínimos vs existentes.....	38
Tabla 3.2 Requerimientos mínimos de Recursos Humanos.....	39
Tabla 3.3 Presupuestos Referenciales	40
Tabla 3.4 Actividades de desarrollo del proyecto	41
Tabla 3.5 Etapas de la metodología PMBOK	42
Tabla 3.6 Habilidades PMBOK.....	42
Tabla 4.1 Actividades de Gestión del Proyecto	47
Tabla 4.2 Actividades de Implementación	48
Tabla 4.3 Identificación de riesgos.....	50
Tabla 4.4 Análisis cualitativo y cuantitativo de los riesgos	50
Tabla 4.5 Categorización de riesgos.....	50
Tabla 4.6 Cronograma etapas de gestión e implementación	52
Tabla 4.7 Matriz de calidad	53
Tabla 4.8 Matriz RACI Gestión de la comunicación	53
Tabla 4.9 Detalle de adquisiciones.....	54
Tabla 4.10 Control de calidad	56

Tabla 4.11 Validación y control del alcance	57
Tabla 4.12 Datos de entrada	80
Tabla 4.13 Simulación 1 Karla Riera	81
Tabla 4.14 Simulación 2 Víctor Borja.....	81

RESUMEN

Durante el transcurso de los años vemos como el fraude toma mayor protagonismo a nivel mundial, en este estudio se examina a fondo el fraude y todo lo que desencadena alrededor del mismo.

El fraude no se limita a los hechos de corrupción administrativa o financiero, sino también se relacionan con actos ilícitos como: El hurto, lavado de activos, complot, bullying, acoso, filtro de información confidencial, etc.

El propósito indispensable no es en descubrir los fraudes, sino prevenirlos y detectarlos antes de que se lleven a cabo actos ilícitos.

The Fraud Explorer es una herramienta fundamental en el presente trabajo que se orienta en la minimización de los riesgos en las estaciones de trabajo de los usuarios ya que no poseen un control interno adecuado dando como resultado que los usuarios estén propensos al fraude, el despliegue de The Fraud Explorer ayudará a este proyecto a que dichas falencias puedan disminuir y poder proporcionar información a la Gerencia General cuando necesite comprobar o prevenir un fraude de sus colaboradores.

Palabras clave: Fraude, corrupción, hurto, lavado de activos, The Fraud Explorer, riesgos.

ABSTRACT

Over the course of the years we see how fraud takes center stage worldwide, in this study we examine in depth the fraud and everything that unleashes around it.

The fraud is not limited to acts of administrative or financial corruption, but also relates to unlawful acts such as: Theft, money laundering, plotting, bullying, harassment, confidential information filter, etc.

The essential purpose is not to discover fraud, but to prevent and detect it before illegal acts are carried out.

The Fraud Explorer is a fundamental tool in the present work that focuses on the minimization of risks in users' workstations since they do not have adequate internal control resulting in users being prone to fraud, the deployment of The Fraud Explorer will help this project so that these shortcomings can diminish and provide information to the General Management when it needs to check or prevent fraud from its collaborators.

Key words: Fraud, corruption, theft, money laundering, The Fraud Explorer, risks.

INTRODUCCIÓN

ANTECEDENTES DE LA SITUACIÓN OBJETO DE ESTUDIO

CELCO Cía. Ltda. se dedicada en proveer soluciones de infraestructura tecnológica de alta confiabilidad y amigables con el medio ambiente para todo tipo de empresas desde el 12 de junio de 1978, su operación está centrada en Ecuador con su matriz en la Ciudad de Quito, dos sucursales en la ciudad de Guayaquil y Cuenca, actualmente cuenta con 85 empleados capacitados y certificados en su línea de trabajo profesional.

Actualmente la empresa CELCO cuenta con un departamento de sistemas conformado por tres personas, distribuidos de la siguiente manera 1 en la oficina matriz Quito y 2 en Guayaquil. Ellos se encargan de brindar soporte a todos los usuarios a nivel de hardware y software a pesar de ello no cuentan con una herramienta de detección y prevención de fraude. Los usuarios tienen acceso a información relacionada con costos, importaciones, bases de datos de clientes, márgenes de utilidad, inventarios, manuales de operación y diseño, catálogos y en general toda información considerada por la empresa como crítica y de carácter confidencial.

Los casos de fraude que se han podido evidenciar son los que se detallan a continuación:

- a) Dos asesoras comerciales alteraron la información oficial sobre las características técnicas de un producto sin autorización para cumplir los requerimientos de un cliente del sector público con el objetivo de ganar una comisión económica una vez que adjudicaron la venta el cliente exigió el cumplimiento de la característica modificada, CELCO Cía. Ltda. no pudo cumplir con lo ofertado y su resultado fue sancionado con 5 años de no poder participar en procesos de adjudicación pública provocando cuantiosas pérdidas a la empresa.
- b) Una coordinadora del departamento técnico creó su propia empresa del mismo giro de negocio de CELCO Cía. Ltda. mientras cumplía con su horario laboral ella aprovechaba y atendía a sus clientes, adicionalmente tomó los formatos de cotizaciones de CELCO Cía. Ltda. para usarlos y obtener un beneficio económico adicional al que percibía. El fraude se detectó cuando un cliente

contactó al Gerente Regional para contrastar precios y formatos de elaboración de ofertas.

- c) El jefe del departamento de ventas y el contador se pusieron de acuerdo para convencer a los clientes que son los dueños de la compañía y cobrar las facturas que estaban pendientes con cheques a nombre de ellos, el monto del fraude se estimó en 26.000,00 dólares.

PLANTEAMIENTO DEL PROBLEMA

El control deficiente en la prevención del fraude laboral puede desencadenar acciones como el despido del personal impulsado por sospechas infundadas y sin prueba alguna, mismas que puede desencadenar en juicios laborales que impactarían a la compañía a nivel económico, social y reputacional.

Se busca establecer o definir un mecanismo de control y monitoreo para prevenir el fraude y este sea detectado a tiempo antes de su cometido y dar antecedentes con evidencia suficiente y así apoyar a la Gerencia General en la toma de decisiones que pueden ser: Descontar, despedir o enjuiciar.

JUSTIFICACIÓN

Al prevenir fraude interno la organización se protege de personal con malas intenciones lo que beneficiará a la organización porque no se verá afectada económicamente al separar a sus malos elementos mientras que se evita despedir a personal sin motivos o solo por sospechas injustificadas que lo único que puede desencadenar son demandas laborales perjudicando la imagen de la organización.

Con el despliegue de la herramienta Fraud Explorer se pretende controlar el uso de la infraestructura de los usuarios conectados a la red de la empresa CELCO Cía. Ltda. logrando identificar a los posibles autores o causantes antes de que se cometa el delito.

OBJETIVOS

OBJETIVO GENERAL

Implementar “The Fraud Explorer FTA” en la empresa CELCO Cía. Ltda. como mecanismo de prevención y detección de fraude, utilizando su infraestructura tecnológica a través del monitoreo de los usuarios conectados a la red.

OBJETIVOS ESPECÍFICOS

- Investigar sobre los esquemas de fraude utilizando tecnología, mecanismos de monitoreo, control y prevención, y relevar el marco legal para sancionar este tipo de delitos.
- Analizar los permisos de acceso la información crítica por áreas de la empresa.
- Levantar un universo de riesgo de fraude relacionado con el giro de negocio y aprobación de la Gerencia General.
- Identificar los medios comunes de fraude a través de medios tecnológicos que existen en Ecuador.
- Implementar la herramienta The Fraud Explorer en la red.
- Realizar pruebas y simulaciones para comprobar su funcionamiento.
- Analizar los resultados de las pruebas.

DESCRIPCIÓN DE LOS CAPÍTULOS

El proyecto “Implementación The Fraude Explorer FTA en la Empresa CELCO Cía. Ltda. como Mecanismo de Prevención y Detección de Fraude” – incluye 4 capítulos y 10 anexos.

El capítulo 1, es la fundamentación teórica de la tesis propuesta, “Implementación The Fraude Explorer FTA en la Empresa CELCO Cía. Ltda. como Mecanismo de Prevención y Detección de Fraude”.

El capítulo 2, se detalla el marco metodológico en conjunto con las técnicas de recopilación de información utilizadas.

El capítulo 3, se puntualiza sobre el diagnóstico actual de la empresa CELCO Cía. Ltda., además se describe la factibilidad y metodología del proyecto.

El capítulo 4, se centra en la gestión e implementación de la herramienta “The Fraud Explorer”, pruebas de funcionamiento y presentación de resultados además describimos las conclusiones y recomendaciones.

1 **CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA**

1.1 **ESTADO DEL ARTE**

Entender que convivimos con el fraude en distintas escalas es preocupante como sociedad por ello es clave tener un enfoque estratégico cuando se realiza la gestión del riesgo de fraude, se investigó varios trabajos que pueden servir como base o como punto de partida para la realización del presente proyecto, se obtuvo los siguientes resultados:

En Bogotá se desarrolló el proyecto titulado “Prevención y detección del fraude en el proceso de suministro de equipos en el sector de la construcción y minero”, se enfocó en realizar una guía metodológica para prevenir, identificar e investigar los fraudes en la comercialización de equipos tomando como ejemplo la empresa COL S.A., su objetivo fue disminuir o eliminar las indisciplinas, ilegalidades y manifestaciones de corrupción en los trabajadores y directivos responsables de las compras o adquisiciones en las organizaciones. (Mayorga, 2016)

En Ecuador se realizó el proyecto titulado “Estrategias para prevención de riesgos y fraudes en inventarios mediante técnicas de auditoría forense”, se centró en establecer estrategias para la prevención de riesgos y detección de fraudes en una compañía dedicada a la importación y comercialización de artículos de iluminación y eléctricos. (Mite & Silva, 2017)

María de los Ángeles Soberanis Aguirre de Rueda y Francisco Ernesto Herrera Soria plantearon como tema de tesis “La auditoría interna en la detección y prevención de fraudes” relacionado en control de procesos internos de tal forma que permita reducir hasta su mínima expresión el riesgo de que ocurra el fraude y si llegara a ocurrir, poder detectarlo oportunamente y así determinar tanto el costo como responsabilidad de los defraudadores. (Soberanis & Herrera, 2018)

De acuerdo a lo anteriormente expuesto se realizó una investigación a nivel nacional e internacional donde se encontró trabajos similares al tema propuesto “IMPLEMENTACIÓN “THE FRAUD EXPLORER FTA” EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE” pero se enfocan en auditorías, metodologías y controles que se pueden aplicar dentro de una organización para mitigar o reducir el fraude todos concluyen que es fundamental tener un mecanismo de prevención de fraudes que afectan la estabilidad de las empresas.

1.1.1 FRAUDE

En la actualidad el fraude va ganando terreno a pasos agigantados dentro de las empresas porque cada día resulta más fácil cometerlo, apoyado en gran medida de la tecnología y sus diversas herramientas que disponemos hoy en día, su ejecución cada vez se realiza con mayor rapidez y su detección es más difícil. Todo esto conlleva que los empresarios asuman un mayor riesgo.

El fraude implica una infinidad de actos ilegales y uno de sus objetivos es afectar económicamente a cualquier empresa por más grande o pequeña que esta sea.

El objetivo del fraude es engañar a una persona, empresa u organización en forma intencional, con el propósito de obtener una ventaja injusta en perjuicio de los derechos o intereses de otra persona o entidad. (Gutierrez, 2015)

Según las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna del Instituto de Auditores Internos (IAI por sus siglas en inglés) es denominado fraude:

Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios. (IAI, 2017)

El fraude incluye cualquier acto intencional o deliberado de privar a otro de una propiedad o dinero por la astucia, el engaño, u otros actos desleales. (ACFE, 2014)

El fraude comprende una amplia gama de irregularidades y actos ilegales caracterizados por la intención de engañar o proporcionar falsa información. (Frett, 2014)

La mayoría de la población puede involucrarse en conductas ilegales, en la *Figura 1.1* mostramos en porcentajes de la población usando la regla del 10 80 10.



Figura 1.1 Regla del 10 80 10

Adaptada de: (Alanís, 2017)

Elaborado por el autor

1.1.2 TIPOS DE FRAUDE

a) FRAUDE INTERNO

Conocido como fraude laboral, se puede definir como: "El uso de la ocupación o empleo de uno para el enriquecimiento personal a través del mal uso deliberado o mala aplicación de los recursos o activos de la organización" En pocas palabras, este tipo de fraude se produce cuando un empleado, gerente, o ejecutivo comete fraude en contra de su empleador. Aunque los autores de fraude están adoptando cada vez más la tecnología y nuevos enfoques para conciliar y ocultar las tramas de fraude en el trabajo, las metodologías utilizadas en este tipo de fraudes generalmente se dividen en categorías claras, probadas a lo largo del tiempo. (ACFE, 2014)

b) FRAUDE EXTERNO

El fraude externo contra una compañía cubre una amplia gama de esquemas. Vendedores deshonestos que podrían participar en esquemas de manipulación de licitaciones, facturación a la empresa por bienes o servicios no prestados, solicitudes de sobornos a los empleados. Del mismo modo, los clientes deshonestos podrían presentar cheques sin fondos o información de una cuenta falsificada para el pago, o podrían tratar de devolver los productos robados o rebajados para un reembolso. Además, las organizaciones también se enfrentan a amenazas de violaciones a la seguridad y robos de propiedad intelectual cometidos por terceros desconocidos.

Otros ejemplos de fraudes cometidos por terceros externos incluyen la piratería, el robo de información confidencial, el fraude fiscal, quiebra fraudulenta, fraude a seguros, fraude de atención médica, y el fraude de préstamo. (ACFE, 2014)

c) FRAUDE CONTRA LAS PERSONAS

Numerosos defraudadores también han ideado planes para defraudar a las personas. El robo de identidad, los esquemas de Ponzi, esquemas de phishing, y los fraudes con los pagos por adelantado, son sólo algunas de las formas criminales que se están dando para robar el dinero de las víctimas inocentes. (ACFE, 2014)

Como se manifiesta el fraude está ligado al engaño con el objetivo de tener beneficios ilegales, por tanto, se convierte en un delito.

Los fraudes son ejecutados por una o más personas e incluso empresas enteras con el propósito de tener réditos monetarios, de bienes o servicios; o para obtener beneficios a sus empresas que les represente ventaja sobre la competencia.

Las consecuencias de los fraudes impactan negativamente para las personas y empresas empezando por la pérdida de credibilidad y confianza, ocasionando baja de reputación y su estabilidad en el mercado.

d) FRAUDE FINANCIERO

Las Normas Internacionales de Auditoría (NIA) definen al fraude de la siguiente manera: "Fraude se refiere a un acto intencional por uno o más individuos dentro de la administración, empleados, o terceras partes, el cual da como resultado una representación errónea de los estados financieros."

Según Instituto de Capacitación para el Desarrollo Ejecutivo ICADE dice que *"los casos de fraude financiero son muchos y muy variados, a manera de ejemplo se mencionan los siguientes"*:

- Alteración de registros.
- Apropiación indebida de efectivo o activos de la empresa.
- Apropiación indebida de los ingresos de la empresa mediante el retraso en el depósito y contabilización de los mismos
- Defraudación fiscal.

- Inclusión de transacciones inexistentes (falsas).
- Lavado de dinero y activos
- Ocultamiento de activos, pasivos, ingresos, gastos.
- Omisión de transacciones existentes.
- Pérdidas o ganancias ficticias.
- Sobre o sub valoración de cuentas.
- Sobre valoración de acciones en el mercado.

e) CORRUPCIÓN

Esta categoría de fraude encuadra todas aquellas actividades en donde los empleados de una empresa utilizan indebidamente sus influencias para obtener un beneficio personal. (ACFE, 2014)

En la *Figura 1.2* observamos las diferentes aristas que se desencadena desde la corrupción.

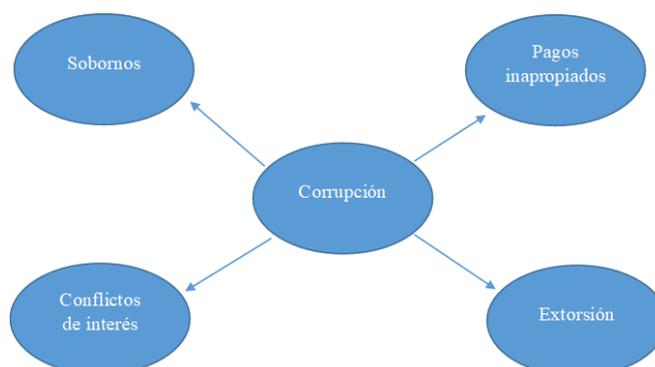


Figura 1.2 Elementos de la Corrupción
Fuente: Elaboración propia

La Organización de Transparencia Internacional (OTI) realiza diversas investigaciones a una base de 180 países donde los clasifica por sus índices de corrupción en una escala desde 100 es libre de corrupción y 0 es considerado altamente corrupto, a continuación, detallamos a nivel de Sudamérica un resumen de la clasificación.

Tabla 1.1 Clasificación de percepción de corrupción

Puesto 2017	País	Abreviatura	CPI Puntaje / 100
23	Uruguay	URY	70
26	Chile	CHL	67
77	Suriname	SUR	41
85	Argentina	ARG	39
91	Guyana	GUY	38
96	Brasil	BRA	37
96	Colombia	COL	37
96	Perú	PER	37
112	Bolivia	BOL	33
117	Ecuador	ECU	32
135	Paraguay	PRY	29
169	Venezuela	VEN	18

Adaptado de: (Transparency International, 2018)

Elaborado por el autor

1.1.3 MODELOS DE FRAUDE

Los perpetradores explotan principalmente deficiencias de los controles internos para su propio beneficio, lo que resulta en daños sustanciales a la organización. El estafador típico es un varón de mediana edad, empleado por la organización de una serie de años. (Control Interno y Fraudes, 2006)

Frecuentemente labora en un área crítica de la organización como el departamento financiero, comercial, logística o técnico, inducido por la ambición de obtener un beneficio económico. Según estadísticas a nivel mundial los fraudes son cometidos por personas con cargos altos dentro de la empresa puesto que tienen acceso a la información confidencial y tienen menos personas que los supervisan.

El perfil del actor del fraude suele estar en posiciones de confianza para los socios y Presidente de la organización de tal manera que sus objetivos de perpetrar actos indebidos en la organización, se vuelven imperceptibles y puede significar gran inversión de tiempo y costo detectar este inconveniente sin la herramienta o conocimiento correcto.

a) TRIÁNGULO DEL FRAUDE

Es un modelo propuesto por Donald Cressey aproximadamente por el año 1950 en EEUU donde él se desempeñaba como criminologista y decidió realizar un estudio para comprobar que motiva a las personas a cometer fraudes.

“Las personas de confianza se convierten en violadores de confianza cuando se conciben a sí mismos teniendo un problema financiero que no es compartible, son conscientes de que este problema puede ser resuelto en secreto violando la posición de confianza y son capaces de aplicar a su propia conducta en esa situación, verbalizaciones que les permitan ajustar sus concepciones de sí mismos como personas de confianza”, con sus concepciones de sí mismos como usuarios de los fondos o propiedades encomendadas. (Cressey, 2017)

En la Tabla 1.2 describimos cada uno de los elementos del triángulo del fraude propuesto por Donald Cressey.

Tabla 1.2 Elementos del Fraude

Elementos del Triángulo del Fraude	
PRESIÓN	Es el primer componente del triángulo del fraude, es lo que motiva el crimen en primera instancia. El individuo tiene problemas y no es capaz de resolverlos a través de acciones legítimas, por ello, empieza a considerar el cometer un acto ilegal, como robar dinero o falsificar estados financieros y ve en ellos una salida para resolver su problema.
OPORTUNIDAD	Es el segundo componente del triángulo del fraude y se basa en la oportunidad que puede percibir una persona para cometer el crimen. El individuo debe tener alguna manera en la que su posición de confianza le pueda facilitar el cometer un abuso y así poder solucionar su problema, p.e. financiero, con un riesgo muy bajo de ser detectado.
RACIONALIZACIÓN	Es el tercer y último componente del triángulo del fraude y es donde la mayoría de los individuos fraudulentos que no tienen un pasado criminal caen. Ellos se ven como personas honestas, ordinarias y se justifican a sí mismos el acto ilegal como una manera correcta y necesaria de salir de sus problemas.

Adaptado de: (Ríos, 2018)

Elaborado por el autor

b) DIAMANTE DEL FRAUDE

Cabe recalcar que el diamante del fraude no es una teoría con estudios e investigaciones como es la teoría del triángulo del fraude por Donald Cressey. En varios libros y seminarios difieren en los criterios sobre este modelo de fraude donde se agrega un cuarto elemento llamado “capacidad” a los existentes en la propuesta de Cressey; Presión, Oportunidad y Justificación.

El factor "capacidad" que se concibe como los conocimientos y habilidades intelectuales necesarias que debe tener una persona para cometer un fraude, indicando que "el defraudador puede sentir presión, justificar su situación y tener la oportunidad, pero si no tiene la capacidad no podrá llevar a cabo el fraude". (Auditool, 2017)

A continuación, en la *Figura 1.3* se observa los diferentes elementos del diamante del fraude.

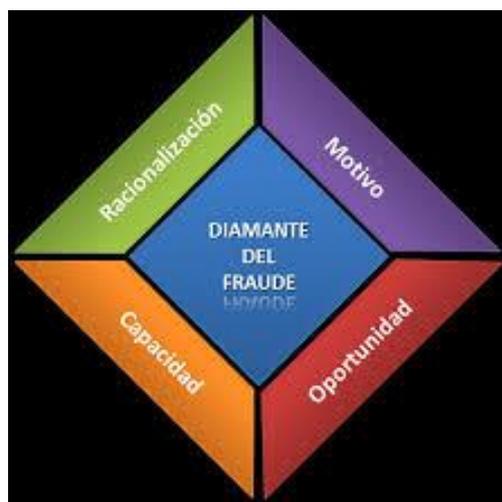


Figura 1.3 Diamante del Fraude
Fuente: (Alanís, 2017)

1.1.4 TÉCNICAS DE FRAUDE UTILIZANDO EQUIPOS DE CÓMPUTO

a) SALAMI

La técnica de Salami consiste en sustraer pequeñas cantidades (tajadas) de un gran número de registros, mediante la activación de rutinas incluidas en los programas aplicativos corrientes. La empresa es la dueña del Salami (archivo de datos) de donde el defraudador toma pequeñas sumas (centavos) para llevarlos a cuentas especiales conocidas solamente por el perpetrador del fraude. Aquí, normalmente, los totales de control no se alteran en consecuencia, se dificulta descubrir al fraude y a quién lo comete.

La técnica de Salami es muy común en los programas que calculan intereses, porque es allí en donde se facilita la sustracción de residuos que generalmente nadie detecta, configurándose cómodamente el fraude. (Estupiñan, Control Interno y Fraudes, 2006)

b) CABALLO DE TROYA

La técnica del Caballo de Troya consiste en insertar instrucciones, con objetivos de fraude, en los programas aplicativos, de manera que, además de las funciones propias del programa, también ejecute funciones no autorizadas.

Las instrucciones fraudulentas se esconden dentro de las demás, obteniendo acceso libre a los archivos de datos, normalmente usados por el programa.

Esta técnica es muy común debido a la facilidad que se presenta para ocultar las instrucciones fraudulentas dentro de cientos de instrucciones que generalmente componen los programas aplicativos. Sin embargo, no siempre la técnica del caballo de troya se configura en programas de aplicación, también se acostumbra en sistemas operacionales y en programas utilitarios. (Control Interno y Fraudes, 2006)

Para efectos de incluir la instrucción en un programa legítimo, el programador aprovecha la autorización para hacer cambios corrientes a los programas y en ese momento incluye las instrucciones fraudulentas, evidentemente no autorizadas. A esto se debe que la técnica haya adoptado el nombre de *caballo de troya*. (Estupiñan, Control Interno y Fraudes, 2006)

c) BOMBAS LÓGICAS

Las bombas lógicas son una técnica de fraude, en ambientes computarizados, que consiste en diseñar e instalar instrucciones fraudulentas en el software autorizado, para ser activadas cuando se cumpla una condición o estado específico. Esta técnica de fraude informático, es difícil de descubrir, porque mientras no sea satisfecho la condición o estado específico, el programa funciona normalmente procesando los datos autorizados sin arrojar sospecha de ninguna clase.

Cuando la condición de fraude se cumple, entonces automáticamente, se ejecuta la rutina no autorizada produciéndose de ésta manera fraude. Entre las condiciones más frecuentes, para la práctica de este tipo de fraude tenemos: abonar un crédito no autorizado a una cuenta cuando el reloj del computador alcance determinado día y hora. Hacer un traslado de fondos cuando el computador encuentre una determinada condición como por ejemplo una fecha.

Esta técnica de fraude se diferencia de la del Caballo de Troya, básicamente, en que la instrucción o instrucciones fraudulentas se incluyen en el programa, cuando se está generando originalmente el sistema. En cambio, en el Caballo de Troya, se incluyen las instrucciones fraudulentas cuando es autorizada una modificación al programa.

Esto es, que se ejecutan las modificaciones autorizadas y se aprovecha la oportunidad para agregar instrucciones fraudulentas. (Estupiñan, Control Interno y Fraudes, 2006)

d) JUEGO DE LA PIZZA

El Juego de la Pizza es un método relativamente fácil para lograr el acceso no autorizado a los Centro de Datos. Consiste en que un individuo se hace pasar por la persona que entrega la pizza y en esa forma se garantiza la entrada a las instalaciones del Centro de Datos durante y después de las horas de trabajo. (Estupiñan, Control Interno y Fraudes, 2006)

e) INGENIERÍA SOCIAL

Esta técnica consiste en planear la forma de abordar a quienes pueden proporcionar información valiosa o facilitar de alguna manera la comisión de hechos ilícitos. Se recurre luego, a argumentos conmovedores y/o sobornar a las personas para alcanzar los objetivos deseados.

“Esta técnica combina las características del petulante y del jactancioso para conseguir el hecho fraudulento. Además, normalmente, usan un estilo de actuación importante, vestido elegante, amenazas sutiles y porciones aisladas de información clave de la organización para influir en la otra persona”. (Control Interno y Fraudes, 2006)

1.1.5 SEGURIDAD DE LA INFORMACIÓN

“La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización”. (Costas, 2014)

La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información, mientras que la rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida. (Escrivá, Romero, Ramada, & Pérez, 2012)

Los avances de las Tecnologías de la Información y Comunicación (TIC) han ocasionado que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias

instituciones y minimizar riesgos derivados de vulnerabilidades informáticas. (LEXIS, 2013)

a) INFORMACIÓN

La información es una agrupación de datos relacionados y ordenados de manera que resultan útiles para realizar alguna actividad y tomar decisiones. (Vasconcelos, 2014)

b) TIPOS DE INFORMACIÓN

A continuación, en la Tabla 1.3 resumimos los tipos de información:

Tabla 1.3 Tipos de información

Tipo	Descripción
Privilegiada	Se considera este tipo de información que solo tiene acceso un conjunto de personas determinadas dentro de la organización. Por consiguiente se considera información no pública y su conocimiento es exclusivo.
Publica	Esta información está abierta para todos los colaboradores de la empresa. Por lo tanto está disponible para conocimiento de todos.
Confidencial	Se considera información oculta y no está disponible para todo el público sino para un grupo muy limitado de personas. Por lo general esta información es considerada como crítica y significativa
Externa	Esta información estará disponible una vez que se autorice su publicación, su objetivo de creación es para un fin determinado.
Interna	Este tipo de información se administra a la interna de una organización o de un grupo de personas. Su particularidad es que solo es de interés a esas personas.
Personal	Es el conjunto de datos que nos indica atributos y características sobre una persona específica.

Fuente: Elaboración propia

1.1.6 RIESGO

Es indiscutible que a diario estamos en riesgo informático, los avances tecnológicos nos otorgan innumerables beneficios para nuestro entorno laboral, económico, social y académico, por tal motivo existe una gran maza de usuarios que acuden a ella en busca de conseguir estos servicios tecnológicos, es por ello que en la red existe una enorme cantidad de información de dichos usuarios que se registran e ingresan información personal día tras día y segundo a segundo.

TIPOS DE RIESGOS INFORMÁTICOS

a) AMENAZAS INTERNAS

“La reciente publicación de WikiLeaks de los cables diplomáticos clasificados del Departamento de Estado de EE.UU. es un excelente ejemplo de los ataques maliciosos internos”. (Ernst & Young, 2011)

Las amenazas internas comúnmente se enfocan en el cometimiento de delitos como: Robos, violación de la propiedad intelectual, espionaje comercial y daños directos que pueden ocasionar trabajadores disgustados contra la organización pudiendo afectar la estabilidad económica y reputacional de la compañía.

b) COMPUTACIÓN EN LA NUBE

“En un mundo tan complejo como el de la nube, la movilidad y las redes sociales, las amenazas que originan los usuarios internos o los usuarios externos haciéndose pasar por internos son especialmente dañinas. Esto es particularmente cierto cuando los usuarios internos acumulan una gran cantidad de derechos de acceso con privilegios. Controlar el acceso y supervisar los cambios en sistemas y activos críticos resulta clave para reducir las posibles amenazas” (NetIQ, 2016).

La mayor amenaza en la computación en la nube recae en el tipo de servicio que se tenga contratado, muchas empresas no toman en cuenta las cláusulas del servicio que van a recibir y sus condiciones, por ejemplo, la responsabilidad de los backups puede ser potestad del proveedor o de la empresa contratante todo dependerá del modelo de contrato de servicio, adicionalmente los accesos no autorizados pueden incitar al robo o eliminación de información crítica para la organización.

c) REDES SOCIALES

Ahora más que nunca las personas recurren a las redes sociales. A medida que evoluciona la tecnología, las líneas entre las interacciones personales y profesionales se vuelven menos claras. (Ernst & Young, 2011)

Las redes sociales en la actualidad han pasado a ser parte de nuestra vida personal y social dejando canal de comunicación abierto para generar oportunidades de delitos como: El fraude, corrupción, ciber acoso, grooming, sexting, etc.

1.1.7 REGULACIÓN LOCAL PARA DELITOS INFORMÁTICOS

a) CÓDIGO INTEGRAL PENAL (COIP)

La Asamblea Nacional del Ecuador como máximo organismo dentro de la función legislativa el 3 de febrero de 2014, discutió y aprobó el CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP). (Asamblea Nacional, 2014)

En la *Figura 1.4* se muestra un mapeo de los delitos asociados al fraude con su respectivo tiempo de reclusión que va desde los 6 meses hasta los 7 años. Para mayor detalle de los artículos que sancionan el fraude y los delitos relacionados al mismo revisar Anexo 1. Código Orgánico Integral Penal.

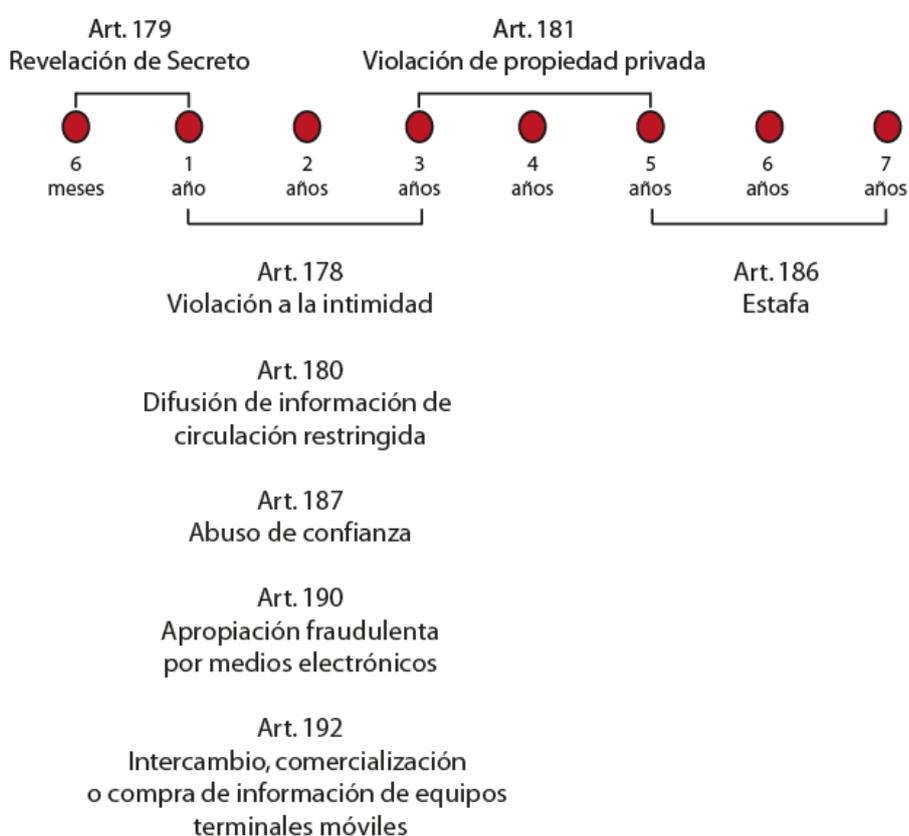


Figura 1.4 Mapeo Delitos COIP
 Adaptado de: (Ministerio de Justicia, 2017)
 Elaborado por el autor

b) CÓDIGO DEL TRABAJO

El 26 de septiembre del 2012 se realiza la última modificación al código del trabajo a cargo de la comisión de legislación y codificación con la finalidad de mantener actualizada la legislación laboral. Los artículos que contemplan sanción a través del código del trabajo se detallan a continuación.

Tabla 1.4 Código del Trabajo

Artículo	Descripción
172	<p>Causas por las que el empleador puede dar por terminado el contrato</p> <p>Por indisciplina o desobediencia graves a los reglamentos internos legalmente aprobados;</p> <p>Por injurias graves irrogadas al empleador, su cónyuge o conviviente en unión de hecho, ascendientes o descendientes, o a su representante</p>
183	<p>Calificación del visto bueno</p> <p>En los casos contemplados en los artículos 172 y 173 de este Código, las causas aducidas para la terminación del contrato, deberán ser calificadas por el inspector del trabajo, quien concederá o negará su visto bueno a la causa alegada por el peticionario, ciñéndose a lo prescrito en el capítulo "Del Procedimiento". La resolución del inspector no quita el derecho de acudir ante el Juez del Trabajo, pues, sólo tendrá valor de informe que se lo apreciará con criterio judicial, en relación con las pruebas rendidas en el juicio.</p>

Adaptado de: (Ministerio de Justicia, 2012)

Elaborado por: El autor

c) **REGLAMENTO INTERNO DE TRABAJO CELCO CÍA. LTDA.**

En Quito el 13 de noviembre de 2013 la Dirección Regional del Trabajo y Servicio Público en cumplimiento de lo dispuesto por el artículo 64 del Código del Trabajo en vigencia, así como, lo prescrito en el numeral 12 del artículo 42 del mismo cuerpo legal, y en general para la mejor observancia de las disposiciones sobre el trabajo, "CELCO Cía. Ltda.", aprobó el Reglamento Interno de Trabajo que regirá aspectos administrativos, disciplinarios y operativos de la Empresa. Ver Anexo 2. Reglamento Interno de Trabajo CELCO Cía. Ltda.

1.2 **LÓGICA DEL NEGOCIO**

CELCO Cía. Ltda. abrió sus puertas hace 40 años y es pionera en la comercialización de equipos para protección eléctrica en el Ecuador, ha diversificado sus productos y líneas de negocio actualmente cuenta con equipos para Centros de Cómputo como: Detección y Extinción de Incendios, CCTV, Aire Acondicionado de Precisión, Piso Técnico, sistemas biométricos, etc.

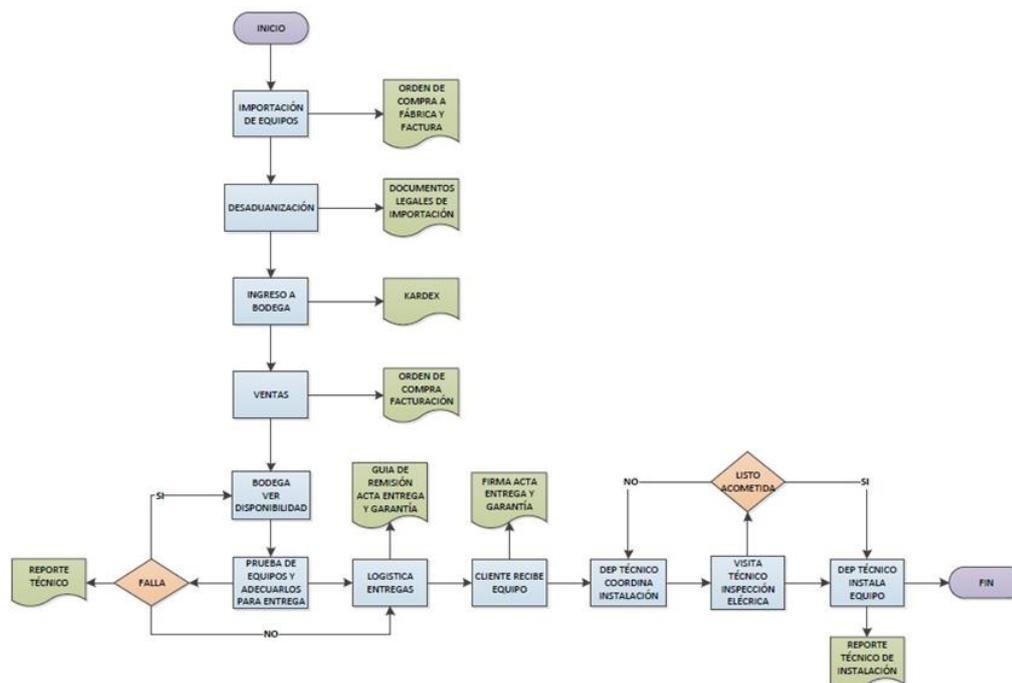


Figura 1.5. Diagrama de flujo proceso de comercialización
Fuente: Elaboración propia

1.2.1 LINEAS DE NEGOCIO

A continuación en la Tabla 1.5 detallamos las líneas de negocio que comercializa y ofrece la empresa CELCO Cía. Ltda.

Tabla 1.5 Catálogo de productos

Catálogo de productos		
Ítem	Línea de negocio	Productos
1	Centros de cómputo	UPS Sistemas Ininterrumpibles de Potencia, de marcas confiables TVSS, protegen de picos provenientes de la red eléctrica pública Baterías de Ciclo Profundo para UPS y para Telecomunicaciones Acondicionadores de Aire de Alta Precisión Sistemas para Detección y Extinción de Incendios Piso Falso, CCTV (Circuito Cerrado de TV) Lectores para Acceso biométrico Puertas para Seguridad y contra fuego PDU, MUD (Power Distribution Unit) Plantas DC, rectificadores, e Inversores
2	Telecomunicaciones	Baterías de Ciclo Profundo para UPS y para Telecomunicaciones Inversores Tableros Eléctricos para media y baja tensión Transferencias ATS/ATO

		STS (Static Transfer Switch)
		Soluciones Software, Plataformas inteligentes.
		Paneles para Operación Remota
3	Energías Renovables	Paneles Solares
		Turbinas Eolicas
4	Maquinaria Industrial	Maquinaria Industrial; Purificación de agua
		Maquinaria para fabricación de hielo
		Maquinaria para elaboración de alimentos, otras
5	Mantenimientos	Mantenimiento preventivo programado
		Mantenimiento correctivo y en emergencia, 24/7
		Turbinas a Gas
6	Otros	Turbinas hidráulicas para Generación Eléctrica
		Redes Eléctricas, cableado estructurado (Redes Voz y Datos) y Fibra Óptica
		Iluminación LED y a Inducción

Adaptada de: (CELCO Cía. Ltda., 2018)

Elaborado por el autor

1.3 HERRAMIENTAS TÉCNICAS

1.3.1 COMPONENTES DE LA SOLUCIÓN

La herramienta “The Fraud Explorer” tiene varios componentes, que trabajando en conjunto hacen viable que el modelo de fraude basado en el triángulo del fraude con inteligencia artificial, a continuación, los describimos.

Tabla 1.6 Componentes de The Fraud Explorer

Nro.	Componente	Descripción
1	Agente o Endpoint	Software que se instala en cada máquina (PC) mediante un .msi que recolecta datos conductuales, desarrollado en .NET C#.
2	Consola web	Aplicación web donde se opera y administra toda la solución, desarrollada en PHP, JavaScript, CSS y HTML.
3	Transformador de datos no estructurados	Logstash es una herramienta de administración de logs que recolecta los datos enviados por el agente .msi, los parsea y envía a Elasticsearch.
4	Almacenamiento y motor de búsqueda	Elasticsearch es el motor de almacenamiento que indexa y analiza los datos enviados por el agente .msi y parseados a través de Logstash.
5	Base de datos SQL	MariaDB es la base donde residen los datos que se consultan de forma inmediata a través de la consola web. A menudo, el procesador de alertas envía datos de Elasticsearch a MariaDB.

6	Procesador de alertas y AI	Busca asociaciones del triángulo del fraude, calcula y alimenta la base de datos SQL. Luego, aplica inteligencia artificial a través de un motor de inferencia.
---	----------------------------	---

Fuente: (NF Cybersecurity and Antifraud Firm S.A.S, 2019)

1.3.2 CONCEPTUALIZACIÓN

Tabla 1.7 *Conceptualización*

Objeto	Descripción
Agentes o Endpoints	El agente es un software desarrollado en .NET y se ejecuta en modo silencioso en cada estación de trabajo de los usuarios que laboran bajo una infraestructura de red corporativa, su objetivo de acuerdo a su programación es enviar datos al servidor para su posterior análisis.
Objetos de políticas de grupo	Se compone de un conjunto de reglas que controlan el entorno de trabajo las cuentas de usuario y de equipo. Las directivas de grupo son comúnmente encontradas en ambientes corporativos entre su principal función es gestionar de manera centralizada los sistemas operativos y aplicaciones de los usuarios registrados en dicha directiva.
Framework .NET	Microsoft diseño este framework haciendo énfasis en la transparencia de redes, brindando independencia de recursos a nivel de hardware y que permite un ágil diseño de aplicaciones, es común que los sistemas operativos basados en Windows tengan preinstalado este framework.
Librería de frases	La librería de frases es el corazón del sistema de detección de conductas sospechosas y de ella depende que se tengan buenos o malos resultados que se obtengan al finalizar el análisis respectivo.

Adaptado de: (NF Cybersecurity and Antifraud Firm S.A.S, 2019)

Elaborado por el autor

1.4 ALTERNATIVAS DE SOLUCIÓN

A continuación, realizamos un cuadro comparativo de alternativas para el monitoreo de las actividades del usuario con el objetivo de detectar y prevenir amenazas internas dentro de una empresa.

Tabla 1.8 *Soluciones Alternativas*

	Ekran System®	Observeit	Veriato 360	The Fraud Explorer
Orientado a empresas	Grandes, medianas y pequeñas	Grandes	Grandes, medianas y pequeñas	Grandes, medianas y pequeñas
Precio	\$6.500,00	\$27.500,00	\$5.073,00	\$0,00
Biblioteca de palabras	Si	Si	Si	Si
Sistema Operativo Servidor	Windows, Linux, Mac, Citrix	Windows Android iPhone/iPad Mac	Linux	Linux

Base de datos	MySql, Firebird, SQL Server	SQL Server	SQL Server	MariaDB
Soporte	Si	Si	Si	Si
Sistema Operativo Clientes	Windows, Linux y MAC	Windows, Linux y MAC	Windows y Linux	Windows y Linux
Monitoreo en tiempo real	Si	Si	Si	Si
Notificaciones y alertas	Si	Si	Si	Si
Reportes	Sistema avanzado de generación de reportes	Sistema avanzado de generación de reportes	Sistema avanzado de generación de reportes	Sistema estándar de generación de reportes
Año de Fundación	2013	2006	1998	2016
Origen	EEUU	Israel	EEUU	Colombia
Principales clientes	Delloite, UPS, Seoul National University	Asociación Automovilística Estadounidense y Fondo de Pensiones y Cesantías en Colombia	Bridgestone, SONY, Amway, TaskUs, GRUMMAN	Gobierno de Colombia

Fuente: Elaboración propia

Después de una revisión y comparación de las características y beneficios de cada una de las herramientas de monitoreo y prevención de fraude que existen en el mercado se optó por la herramienta The Fraud Explorer considerando que es el único software Open Source que no tiene un costo por licenciamiento que la empresa CELCO Cía. Ltda. no está dispuesta a invertir.

2 CAPÍTULO II. MARCO METODOLÓGICO

2.1 TIPO DE INVESTIGACIÓN

El tipo de investigación es cuantitativo porque se presentan reportes con indicadores numéricos con puntajes asignado por el algoritmo de Donald Cressey y previamente configurados por el administrador de Sistemas que representan el nivel de riesgo de cada usuario conectado a la red de la empresa CELCO Cía. Ltda. que estará monitoreado a través de la herramienta The Fraud Explorer.

El proyecto se desarrolló utilizando la metodología científica, considerando sus etapas y la información recolectada para implementar herramientas de monitoreo y prevención de fraude dentro de las organizaciones.

Tabla 2.1 Etapas de la metodología científica

Etapas	Descripción
Observación	Examinar con atención los antecedentes de fraude cometidos en perjuicio a la empresa CELCO Cía. Ltda.
Hipótesis	Establecer una hipótesis de los hechos encontrados y sus posibles causas
Experimentación	Implementar la herramienta para la prevención y monitoreo de fraude "The Fraud Explorer y observar las acciones que desencadene al cometimiento de delitos dentro de la organización modificando las circunstancias que se consideren convenientes.
Conclusiones	Comprobar e interpretar los resultados arrojados por la herramienta implementada en la red de la empresa CELCO Cía. Ltda.

Fuente: Elaboración propia

2.2 RECOPIACIÓN DE INFORMACIÓN

2.2.1 TÉCNICAS DE RECOPIACIÓN DE INFORMACIÓN

a) ENTREVISTA

Se considera a la entrevista como una pieza de la interacción social donde una persona responde a una serie de preguntas sobre un tema específico, en sí representa una interacción cara a cara entre dos o más personas. La entrevista representa una de las mejores técnicas de recolección de información. Las respuestas que se obtienen pueden ser registradas por medios electrónicos o por escrito. (Avila, 2004)

Se optó por esta técnica de recolección de información porque se analizó a que personas dentro de la empresa CELCO Cía. Ltda. les puede interesar la implementación de una herramienta de prevención y monitoreo de fraude y se concluyó que el beneficio principal lo tendrían las personas que ocupan los cargos más altos dentro de la organización por lo tanto se eligió a la Sra. Diana Fernández Gerente General y al Sr. Santiago Arroyo Accionista de la compañía.

Las encuestas aplicadas a la CEO y Accionista de la compañía CELCO Cía. Ltda. se encuentran disponibles en el Anexo 3. Entrevistas.

➤ ANÁLISIS DE LAS ENCUESTAS

La gerencia general y uno de los accionistas concuerdan que el fraude es un tema crítico dentro de cualquier organización, los resultados de la entrevista arrojan argumentos suficientes para identificar las causas, efectos y consecuencias de un posible fraude y como se enfrentarían estos problemas dentro la empresa.

En el marco de revisión bajo la información recabada, se destaca el compromiso por parte de la alta gerencia, que busca solventar esta necesidad de forma inmediata y así evitar cualquier fraude que perjudique los intereses de la empresa y sus accionistas, sin embargo, la implementación es un tema pendiente que debe consensuarse con todas las partes interesadas de la organización, además de socializarlos paulatinamente para detectar fisuras en el proceso y que el delito pueda ser identificado de forma clara y rápida.

Para tener un mejor panorama en este aspecto, los métodos que se utilicen en la gestión de cambio y sobre todo en la implementación del sistema deben ser amigables, sencillos y de un alto compromiso y responsabilidad que determinen una actuación a conciencia y ética por parte de sus actores asumiendo este encargo con imparcialidad.

Se recomienda iniciar de inmediato con la planificación y un cronograma para la implementación del sistema, además de las charlas y capacitaciones de interés que aclaren el panorama empresarial actual y den pautas iniciales para continuar con su ejecución como herramienta útil en la generación de nuevos procesos administrativos necesarios para el correcto funcionamiento de las operaciones organizacionales.

b) ANÁLISIS DE CONTENIDO

El Análisis de Contenido es una técnica que permite reducir y sistematizar cualquier tipo de información acumulado (documentos escritos, films, grabaciones, etc.) en datos, respuestas o valores correspondientes a variables que investigan en función de un problema. (Chavez, 2008)

Para evidenciar los antecedentes de fraude cometidos en la empresa CELCO Cía. Ltda. se revisó la evidencia en el respaldo del servidor de correos y demás documentos físicos que están en poder del departamento legal y se constató los delitos cometidos, gerencia general no autorizó anexar evidencia al presente proyecto por seguridad y

recomendación de los asesores legales de la organización, sin embargo, se presenta un detalle general de la información analizada.

Tabla 2.2 *Resumen Casos de Fraude*

Resumen General de Casos de Fraude				
Nro.	Año	Casos	Área	Estatus
1	2009	1	Financiero	Proceso legal finalizado a favor de la empresa.
2	2012	1	Comercial	Proceso legal en curso.
3	2015	2	Administrativa	No se inició un proceso legal, se despidió a las personas involucradas con acción de visto bueno.
4	2018	1	Técnica	En verificación para proceder con acciones legales.

Fuente: Elaboración propia

3 CAPÍTULO III. PROPUESTA

3.1 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

CELCO Cía. Ltda. desde 1978 comercializa soluciones de infraestructura tecnológica de alta confiabilidad y amigables con el medio ambiente, tomando como objetivo primordial la protección de los equipos electrónicos de todos los problemas eléctricos provenientes de la red pública, parte de su cultura organizacional está definida en la misión, visión y política que se detallan a continuación.

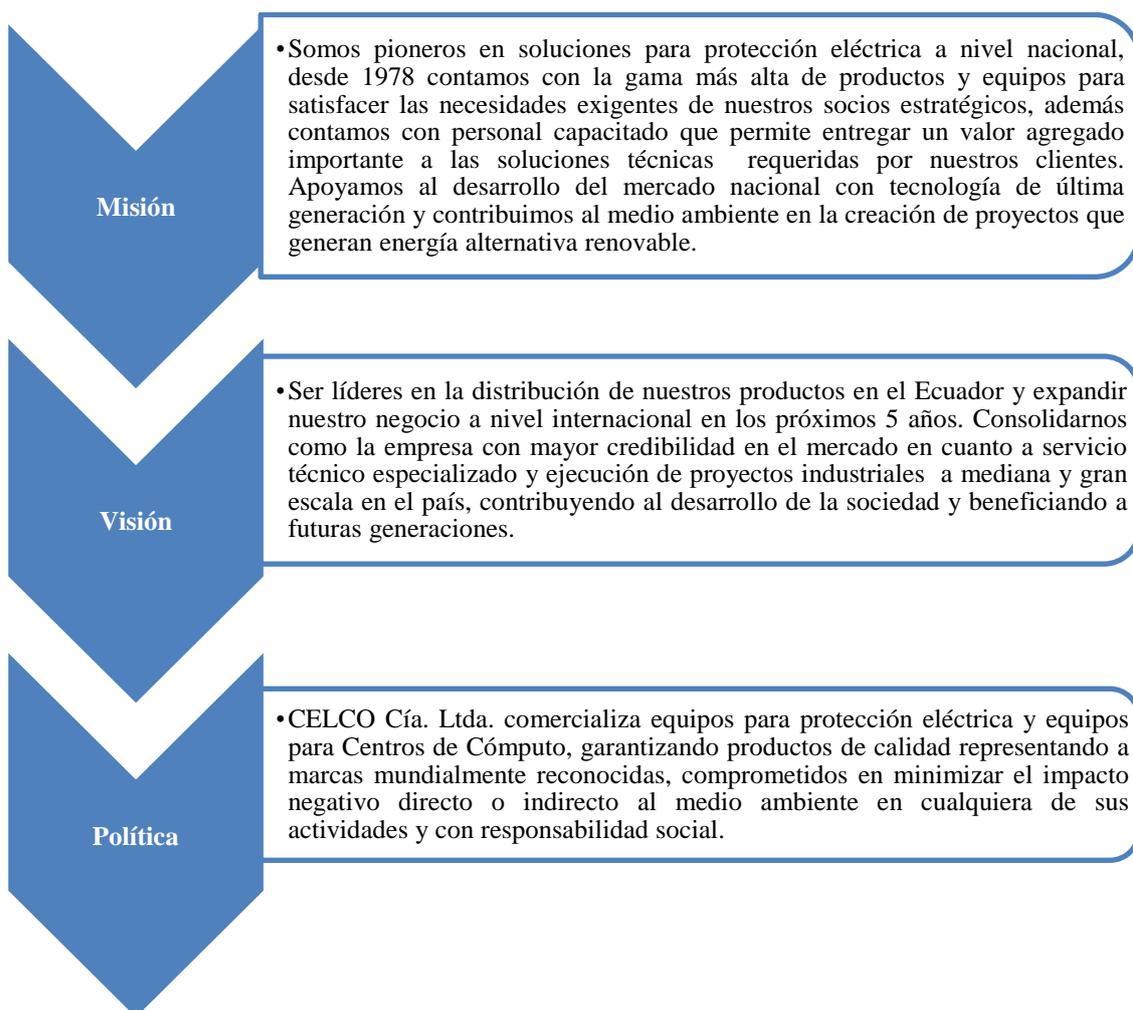


Figura 2.6. Misión, visión y política de CELCO Cía. Ltda.

Adaptado de: (CELCO Cía. Ltda., 2015)

Elaborado por el autor

3.1.1 FACTIBILIDAD TÉCNICA

The Fraud Explorer es un software que necesita requerimientos mínimos para que su ejecución y posterior obtención de resultados sean de manera satisfactoria para las

partes interesadas, a continuación, detallamos las características mínimas a nivel de hardware y software.

Tabla 3.1 Requerimiento mínimos vs existentes

Requerimientos para despliegue de The Fraud Explorer				
Ítem	Equipo	Características	Mínimo	Existentes CELCO Cía. Ltda.
1	Servidor	Marca / Modelo	N/A	HP Provilant
		Procesador	Xeon 1.3 GHz con 4 núcleos, Gen8	Xeon 2.3 GHz con 8 núcleos, Gen9
		Memoria RAM	4GB DDR3 1600 MHz	16GB DDR4 2400 MHz
		Sistema Operativo	Windows Server 2003 en adelante, 32bits o 64bits	Windows Server 2012 R2 64bits
		Disco Duro	2TB	8TB
2	Estación de trabajo	Marca / Modelo	N/A	Lenovo MT 81 CA
		Procesador	Core I3 4ta Gen.	Core I7 8va Gen.
		Memoria RAM	4GB	8GB
		Sistema Operativo	Windows 10 Pro	Windows 10 Pro
		Disco Duro	N/A	512GB SSD

Fuente: Elaboración propia

3.1.2 FACTIBILIDAD OPERACIONAL

La empresa CELCO Cía. Ltda. posee un departamento de Sistemas conformado por 3 personas que se encargan de brindar soporte a nivel de hardware y software a todos los usuarios de la organización, se encuentran distribuidos de la siguiente manera.

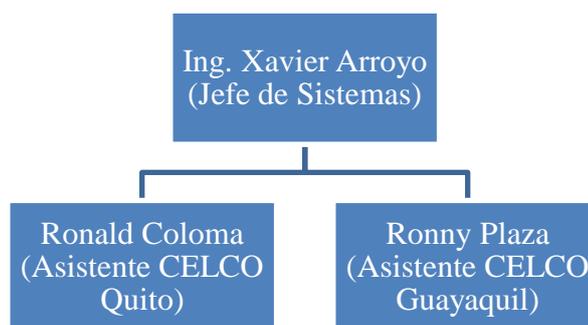


Figura 3.7 Organigrama Departamento Sistemas CELCO Cía. Ltda.

Fuente: Elaboración propia

Una vez realizado el análisis de acuerdo a la experiencia y capacitación que posee cada recurso del departamento de sistemas, se ha distribuido los diferentes roles y actividades a realizar.

Tabla 3.2 Requerimientos mínimos de Recursos Humanos

Requerimientos mínimos Recursos Humanos		
Rol	Actividades	Descripción
Implementador	Instalar la solución, configurarla y mantenerla	Debe existir una persona que se encargue de implementar técnicamente la solución, que tenga conocimientos de infraestructura Linux y programación en PHP.
	Desplegar el Endpoint	Debe existir una persona con conocimientos en infraestructura Windows y Directorio Activo que se encargue de configurar la política GPO para el despliegue del agente en los PC.
Examinador del Fraude	Mantener y mejorar la librería de frases	La librería de frases se debería ajustar a las necesidades y rubro de la corporación. Debe existir un examinador del fraude que entienda la teoría del triángulo de Donald Cressey y ayude a alimentar, mejorar o corregir el diccionario principal que usará The Fraud Explorer para asociar las conductas.
	Establecer rangos de criticidad del fraude	La solución The Fraud Explorer viene con tres categorías de fraude: baja, media, alta y crítica. Cada alerta y puntuación total, así como promedios están definidos por estas categorías, que pueden modificarse en la solución de acuerdo a las necesidades que considere el examinador del fraude.
	Analizar las alertas y comunicar los resultados	El Examinador del Fraude es aquel que analizará las alertas generadas por el software, decidirá si son pertinentes o si son un falso positivo que debe marcar e ignorar. Esta persona deberá comunicar a la organización sobre cualquier alerta verdadera para que se tomen las decisiones administrativas correspondientes, como una investigación dirigida, análisis forense o asistencia legal especializada.

Fuente: Elaboración propia

En el caso de no contar con personal que tengan conocimientos como se detalló en la descripción del perfil se debe optar por contratar o capacitar a por lo menos una persona de la organización en: Administración de Servidores Windows y Linux, Manejo de Servidores Virtualizados, Bases de PHP y Administración de Directorio Activo.

3.1.3 FACTIBILIDAD ECONÓMICA

CELCO Cía. Ltda. al ser una compañía que lleva más de 40 años en el mercado, en años pasados vió la necesidad de incorporar entre sus activos equipos de computación de última generación (servidores), licencias de Microsoft para su respectiva administración y contrató personal calificado en el área de Sistemas para brindar soporte a los usuarios, administrar los servidores y mantener la infraestructura de TI en óptimas condiciones.

A continuación se detalla el presupuesto de CELCO Cía. Ltda. que corresponde al optimista en la Tabla 3.3, donde los costos se reducen a \$0,00 por tener todos los ítems necesarios para el despliegue de la herramienta The Fraud Explorer dentro de su inventario, además se plantea un presupuesto real donde detallamos los valores que tiene cada ítem actualmente en el mercado y para finalizar proyectamos un presupuesto pesimista donde los valores corresponden al precio máximo que se puede encontrar en el mercado tecnológico considerando que no se tendría el apoyo o asesoría de un departamento de Sistemas.

Tabla 3.3 Presupuestos Referenciales

Presupuestos					
Descripción Gasto	Cant.	Subítems	Real	Optimista	Pesimista
	1	Servidor	2.072,00	0,00	3.500,00
	2	Discos Duros	1.062,00	0,00	1.450,00
	2	Memoria RAM 8GB	444,00	0,00	480,00
Materiales	1	Estación de trabajo C/U	450,00	0,00	800,00
	1	Licencia The Fraud Explorer	0,00	0,00	0,00
	1	Licencia Visual Studio 2015	1.139,00	0,00	1.614,00
	1	Licencia Windows Server	760,00	0,00	760,00
	1	Capacitación	450,00	0,00	600,00
		Instalación y configuración Windows Server			
Mano de Obra	1	- Servicio de Active Directory	1.200,00	0,00	1.600,00
		- Servicio DNS			
	1	Sueldo / Mensual	800,00	0,00	1.200,00
Costos Indirectos	1	Movilización	20,00	0,00	20,00
	1	Alimentación	10,00	0,00	10,00
		Total Gastos	8.407,00	0,00	12.034,00

Fuente: Elaboración Propia

3.1.4 MODELO O ESTÁNDAR A APLICAR

La metodología que se eligió para el desarrollo de este proyecto es PMBOK 6ta edición por su capacidad de adaptación, no es necesario que la compañía CELCO Cía. Ltda. cambie su estructura para acomodarse al enfoque que propone PMBOK, permitiendo elegir los procedimientos a ejecutar, la manera de realizarlos, los métodos a usar, etc.

A continuación, se resume las etapas con sus respectivas actividades que recomienda PMBOK en el desarrollo de proyectos.

Tabla 3.4 Actividades de desarrollo del proyecto

Nro.	Etapas	Actividad
1	Integración	Desarrollar el acta de constitución del proyecto
2	Interesados	Identificar a los interesados
3	Integración	Desarrollar el plan para la dirección de proyectos
4	Interesados	Planificar el involucramiento de los interesados
5		Planificar la gestión del alcance
6	Alcance	Recopilar requisitos
7		Definir el alcance
8		Crear EDT / WBS
9		Planificar la gestión del cronograma
10	Cronograma	Definir las actividades
11		Secuenciar las actividades
12		Planificar la gestión de los riesgos
13		Identificar los riesgos
14	Riesgos	Realizar el análisis cualitativo de riesgos
15		Realizar el análisis cuantitativo de riesgos
16		Planificar la respuesta a los riesgos
17	Recursos	Planificar la gestión de los recursos
18	Costos	Planificar la gestión de los costos
19		Estimar los costos
20	Recursos	Estimar los recursos de las actividades
21	Cronograma	Estimar la duración de las actividades
22		Desarrollar el cronograma
23	Costos	Determinar el presupuesto
24	Calidad	Planificar la gestión de la calidad
25	Comunicaciones	Planificar la gestión de las comunicaciones
26	Adquisiciones	Planificar la gestión de las adquisiciones
27		Dirigir y gestionar el trabajo del proyecto
28	Integración	Gestionar el conocimiento del proyecto
29		Gestionar la participación / involucramiento de los interesados
30		Adquirir recursos
31	Recursos	Desarrollar el equipo
32		Dirigir al equipo
33	Comunicaciones	Gestionar las comunicaciones
34	Adquisiciones	Efectuar las adquisiciones
35	Calidad	Gestionar la calidad
36	Riesgos	Implementar la respuesta a los riesgos
37	Integración	Monitorear y controlar el trabajo del proyecto
38		Realizar el control integrado de cambios
39	Interesados	Monitorear el involucramiento de los interesados
40	Cronograma	Controlar el cronograma
41	Costos	Controlar los costos
42	Comunicaciones	Monitorear las comunicaciones
43	Riesgos	Monitorear los riesgos

44	Calidad	Controlar la calidad
45	Recursos	Controlar los recursos
46	Alcance	Validar el alcance
47		Controlar el alcance
48	Adquisiciones	Controlar las adquisiciones
49	Integración	Cierre del proyecto

Adaptado de: (Gascón, Ordenando los 49 Procesos de la Guía PMBOK 6, 2016)

Elaborado por el autor

Tabla 3.5 Etapas de la metodología PMBOK

Nro.	Etapas	Actividad
1	Inicio del proyecto	Desarrollo del Acta de constitución del proyecto Identificación de los interesados
2	Planificación para la gestión del Alcance	Documentación de requisitos Matriz de trazabilidad de requisitos
3	Planificación para la gestión del Cronograma	Diseño de Diagrama de Gantt
4	Planificación para la gestión de los costos	Determinación del presupuesto
5	Ejecución del proyecto	Ejecución en el área de gestión de la Integración
6	Monitoreo y control	La validación del alcance
7	Cierre del proyecto	Informe final

Fuente: (Project Management Institute Inc., 2017)

Elaborado por el autor

A partir de esta metodología podemos desarrollar varias habilidades como vemos a continuación.

Tabla 3.6 Habilidades PMBOK

Habilidades PMBOK		
Ítem	Habilidad	Descripción
1	Liderazgo	En plena era digital, hoy más que nunca el papel de Project Manager debe girar entorno a liderar e impulsar la transformación digital dentro de la empresa. Un buen líder debe saber transmitir esos valores a su equipo y contagiar su motivación por el trabajo y alcanzar los objetivos.
2	Trabajo en equipo	Ser líder no quiere decir que no necesites trabajar en equipo, al contrario, necesitas interactuar con muchos niveles jerárquicos dentro de la empresa y es muy importante saber cómo interactuar con cada uno de ellos para determinar claramente los objetivos y las directrices a seguir.
3	Organización	En gran medida el trabajo del Project Manager es organizar, organizar y organizar. De él dependen la organización de los procesos y actores de los que depende el proyecto, así como realizar una buena organización de los plazos y tiempos de las acciones.
4	Comunicación	Si algo se espera de un Project Manager es que sea un gran comunicador porque una de sus tareas es crear buenos canales de comunicación y asegurar que todos los agentes implicados en el proyecto conozcan y tengan claro su papel dentro de la planificación.

5	Capacidad de gestión de conflictos	Las relaciones interpersonales en la gestión de proyectos es un hecho y es inevitable que puedan surgir conflictos en alguna de las etapas es importante que el Project Manager sepa gestionar este tipo de problemas y actúe como mediador para solventarlos y crear un buen clima de trabajo.
6	Capacidad de delegar	Un buen gestor debe conocer sus propias limitaciones y asumir que es imposible abarcar todo el control. Por esto, es muy importante que adquiera la capacidad de delegar y confiar en sus subordinados respetando sus funciones y motivándolos en su trabajo.
7	Detallista y atento	La calidad del servicio prestado es uno de los principales objetivos a cumplir por el Project Manager, para ello debe ser exigente y atento con los detalles, evaluando en cada momento que se cumplen los estándares de excelencia y ser capaz de identificar qué falla para tomar la decisión oportuna en ese momento.
8	Conocimiento del mercado	Sin duda el proyecto tiene salida al mercado, es labor del Project Manager conocer las tendencias y la competencia que se puede presentar, para ajustar el enfoque de los objetivos hacia el éxito.
9	Orientación de objetivos	Además de marcar los objetivos principales dentro de un mismo proyecto pueden surgir imprevistos. Es muy importante que el Project Manager sepa orientar al equipo con toma de decisiones rápidas y precisas, estableciendo plazos de cumplimiento.

Adaptado de: (Del Campo, 2018)

Elaborado por: El autor

4 CAPÍTULO IV. IMPLEMENTACIÓN

4.1 APLICACIÓN DEL MODELO, ESTÁNDAR O METODOLOGÍA

4.1.1 DESARROLLAR EL ACTA DE CONSTITUCIÓN DEL PROYECTO

Se desarrolla el acta en conjunto con la Gerencia General y Accionistas de la empresa CELCO Cía. Ltda., para mayor detalle revisar Anexo 4. Acta de Constitución de Proyecto.

Por medio de este documento, la Empresa CELCO Cía. Ltda. autoriza formalmente la ejecución del Proyecto, se establecen los requerimientos preliminares que cumplen con las solicitudes de los interesados del Proyecto, según los siguientes considerandos:

Necesidad Gerencial. - Fundamentados en la necesidad de tener una herramienta que controle y monitoree los contenidos escritos por los usuarios conectados en la infraestructura de red de la organización a fin de prevenir el fraude.

Plan Estratégico. - Se desarrolla el Proyecto, para respaldar las metas estratégicas de la compañía la cual tiene como meta la importación y comercialización ética de equipos de protección eléctrica.

4.1.2 IDENTIFICAR A LOS INTERESADOS

Para la iniciación del proyecto: realizo el Acta de Constitución del Proyecto y los detalles del mismo, además se realizó la identificación de los interesados y su caracterización para el proyecto, para mayor detalle referirse al Anexo 5. Registro de Interesados.

4.1.3 PLANIFICAR LA GESTIÓN DEL ALCANCE

En la Gestión del Alcance contiene los procesos necesarios que avalen que el proyecto cumpla exclusivamente con los requerimientos definidos al inicio.

Para el presente proyecto se manejaron dos procesos los cuales se describen a continuación.

- Recopilar Requisitos
- Definir el alcance
- Crear la EDT

Adicional como parte de los entregables de la gestión de alcance está el documento sobre la Matriz de Rastreabilidad de Requisito.

a) RECOPIRAR REQUISITOS

Para la recopilación de los requisitos se realizaron entrevistas a la Gerente General y a uno de los accionistas de la compañía a fin de determinar la problemática actual, para mayor detalle referirse al Anexo 3. Entrevistas.

b) DEFINIR EL ALCANCE

Se describe el alcance del proyecto el cual fue obtenido aplicando técnicas de recolección de información: Entrevistas y análisis de contenidos.

Objetivos del alcance del Proyecto. - “The Fraud Explorer FTA” en la empresa CELCO Cía. Ltda. como mecanismo de prevención y detección de fraude, utilizando su infraestructura tecnológica a través del monitoreo de los usuarios conectados a la red.

Descripción del Alcance del producto.- The Fraud Explorer estará instalado y configurado en un servidor dedicado que cumpla con los requerimientos mínimos expresados en la Tabla 3.1 *Requerimiento mínimos vs existentes*, se desplegará el agente a todos los usuarios a través de la política GPO del Directorio Activo, el acceso al monitoreo se lo presenta en un Dashboard web que requiere autenticarse para su uso, para la parametrización del servidor y/o agregar nuevas palabras a las librerías que vienen por defecto se realizará de acuerdo a la matriz RACI establecida en la Tabla 4.8 *Matriz RACI Gestión de la comunicación*.

c) CREAR EDT

La Estructura de desglose del trabajo cuenta con dos principales procesos:

- Gestión del Proyecto, se compone de los documentos que certifican las entregas a la dirección del proyecto a las áreas de conocimientos que son aplicables al presente proyecto.
- La implementación de “The Fraud Explorer”, considerado que el despliegue de la herramienta será implementado en la infraestructura
- actual de la empresa CELCO Cía. Ltda. con la supervisión de las partes interesadas.

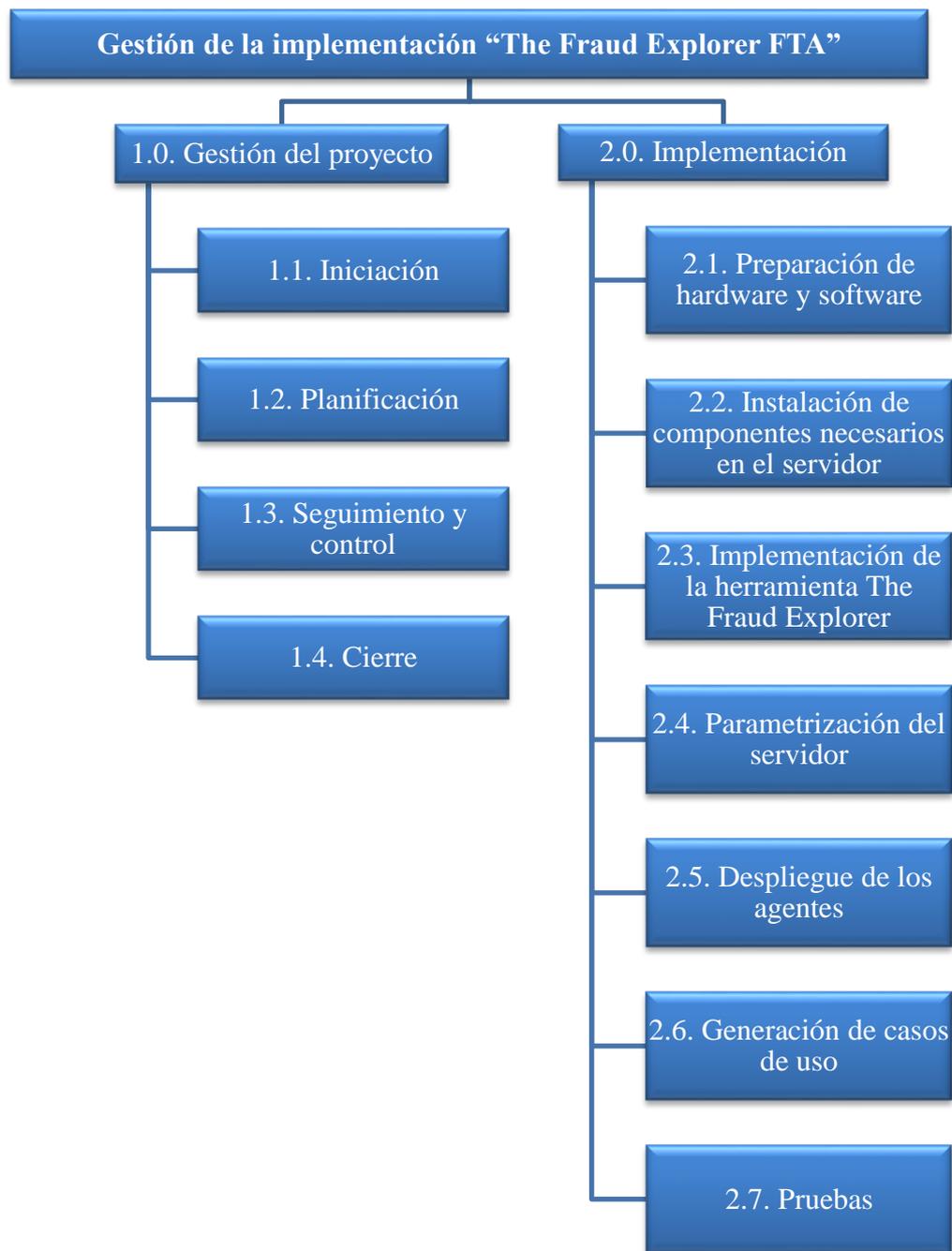


Figura 4.8 Gestión de la implementación
Fuente: Elaboración propia

4.1.4 PLANIFICAR LA GESTIÓN DEL CRONOGRAMA

En la planificación para la gestión del cronograma del proyecto, se realizaron los siguientes procesos:

- Definir las actividades
- Secuenciar las actividades

a) DEFINIR LAS ACTIVIDADES

Para definir las actividades se realizó una evaluación del giro del negocio de la empresa CELCO Cía. Ltda. con las actividades que recomienda la metodología PMBOK 6ta Edición, se decidió utilizar la técnica de descomposición del EDT, a continuación, se detallan las actividades de gestión e implementación del proyecto.

Tabla 4.1 Actividades de Gestión del Proyecto

Nro.	Etapa	Actividades	Si	No	N/A
1	Iniciación del Proyecto	Desarrollar el acta de constitución del proyecto	X		
		Identificar a los interesados	X		
		Desarrollar el plan para la dirección de proyectos			X
		Planificar el involucramiento de los interesados			X
		Planificar la gestión del alcance	X		
		Recopilar requisitos	X		
		Definir el alcance	X		
		Crear EDT	X		
		Planificar la gestión del cronograma	X		
		Definir las actividades	X		
		Secuenciar las actividades	X		
		Planificar la gestión de los riesgos	X		
		Identificar los riesgos	X		
		Realizar el análisis cualitativo de riesgos	X		
		Realizar el análisis cuantitativo de riesgos	X		
		Planificar la respuesta a los riesgos	X		
		2	Planificación	Planificar la gestión de los recursos	X
Planificar la gestión de los costos	X				
Estimar los costos	X				
Estimar los recursos de las actividades	X				
Estimar la duración de las actividades	X				
Desarrollar el cronograma	X				
Determinar el presupuesto	X				
Planificar la gestión de la calidad	X				
Planificar la gestión de las comunicaciones	X				
Planificar la gestión de las adquisiciones	X				
Dirigir y gestionar el trabajo del proyecto	X				
Gestionar el conocimiento del proyecto	X				
Gestionar la participación / involucramiento de los interesados					X
Adquirir recursos					X
Desarrollar el equipo					X
Dirigir al equipo					X
3	Seguimiento y control			Gestionar las comunicaciones	X
		Efectuar las adquisiciones			X
		Gestionar la calidad	X		
		Implementar la respuesta a los riesgos			X
		Monitorear y controlar el trabajo del proyecto	X		

		Realizar el control integrado de cambios	X	
		Monitorear el involucramiento de los interesados		X
		Controlar el cronograma	X	
		Controlar los costos		X
		Monitorear las comunicaciones	X	
		Monitorear los riesgos	X	
		Controlar la calidad		X
		Controlar los recursos		X
		Validar el alcance	X	
		Controlar el alcance	X	
		Controlar las adquisiciones		X
4	Cierre	Cierre del proyecto	X	

Adaptado de: (Project Management Institute Inc., 2017)

Elaborado por el autor

Tabla 4.2 Actividades de Implementación

Nro.	Etapas	Actividades
1	Preparación de hardware y software	Revisar de cumplimiento de requerimientos mínimos. Revisar documentación legal de la herramienta.
2	Instalación de componentes necesarios en el servidor	Instalación de Centos 7 Versión Mínima modo texto.
3	Implementación de la herramienta The Fraud Explorer	Instalación y configuración del servidor The Fraud Explorer.
4	Parametrización del servidor	Parametrizar de acuerdo al giro del negocio.
5	Despliegue de los agentes	Parametrizar y configurar el cosechador Instalar cosechador a través de GPO.
6	Generación de casos de uso	Generar y detectar casos de fraude. Generar y detectar casos de acoso.
7	Pruebas	Emitir reportes con los resultados obtenidos.

Elaboración propia

b) SECUENCIAR LAS ACTIVIDADES

A continuación, se presenta el diagrama de secuencia de las actividades de la gestión del proyecto.

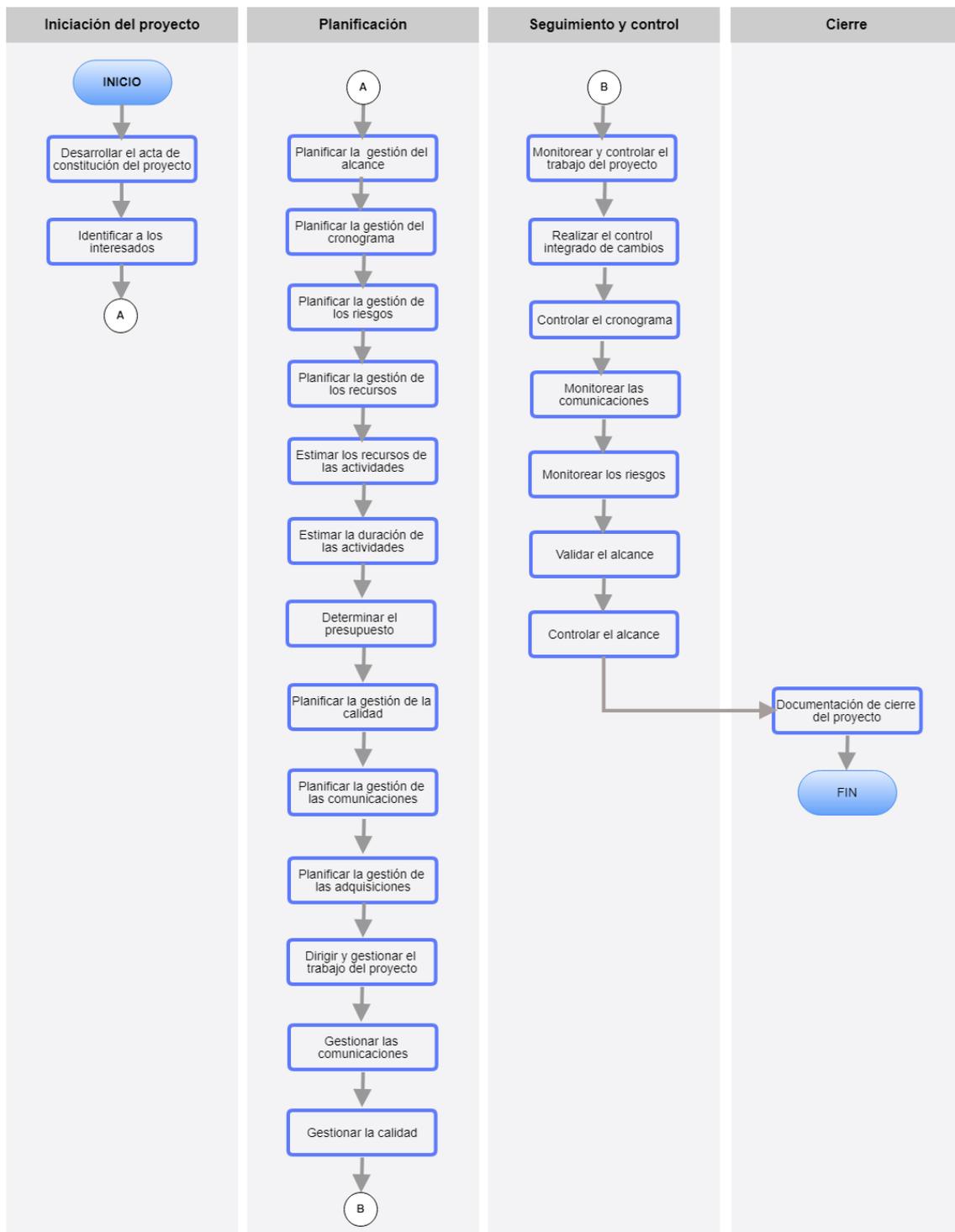


Figura 4.9 Secuencia de Actividades de la Gestión del Proyecto
Fuente: Elaboración propia

4.1.5 PLANIFICAR LA GESTIÓN DE LOS RIESGOS

a) IDENTIFICAR LOS RIESGOS

Los riesgos que comprometen el desarrollo del proyecto o impidan su finalización se los detalla a continuación.

Tabla 4.3 Identificación de riesgos

ID	Causa	Riesgo	Efecto
R01	Personal no especializado en la dirección del proyecto	Incumplir con el alcance, tiempo, costo y calidad	Entregables no aceptados
R02	Implementar la herramienta en una infraestructura inferior a los requerimientos mínimos	The Fraud Explorer no funcione	Molestia por los patrocinadores del proyecto
R03	Malas instalaciones eléctricas en el centro de datos	Los servidores se quemem	The Fraud Explorer no esté operativo
R04	Estimar mal el tiempo	Gerencia General desista del proyecto	Cancelación de la implantación
R05	No existe un control de autenticación de los usuarios a nivel de servidor	La empresa no cuente con un servicio de Directorio Activo	Incurrir en costos de hardware y software para implementar el servicio

Fuente: Elaboración propia

b) REALIZAR EL ANÁLISIS CUALITATIVO y CUANTITATIVO DE RIESGOS

Tabla 4.4 Análisis cualitativo y cuantitativo de los riesgos

ID	Probabilidad (P)	Impacto (I)	Score de riesgo (P*I)
R01	2 (Bajo)	4 (alto)	8
R02	2 (Bajo)	4 (alto)	8
R03	1 (Muy Baja)	5 (Muy alto)	5
R04	3 (Media)	4 (Alto)	12
R05	1 (Muy Baja)	5 (Muy Alto)	5

5: Muy Alta, 4: Alta, 3: Medio, 2: Bajo 1: Muy Bajo

Fuente: Elaboración propia

c) PLANIFICAR LA RESPUESTA A LOS RIESGOS

Tabla 4.5 Categorización de riesgos

		Probabilidad				
		Muy bajo	Baja	Media	Alta	Muy Alta
Impacto	Muy baja	Ignorar	Ignorar	Aceptar	Aceptar	Precaución
	Bajo	Ignorar	Ignorar	Aceptar	Aceptar	Precaución
	Medio	Aceptar	Aceptar	Aceptar	Precaución	Respuesta
	Alto	Precaución	Precaución	Precaución	Respuesta	Respuesta Inmediata
	Muy Alto	Precaución	Precaución	Respuesta	Respuesta	Respuesta Inmediata

Fuente: Elaboración propia

4.1.6 PLANIFICAR LA GESTIÓN DE LOS RECURSOS

En el proyecto no se contempla la integración de nuevos miembros, puesto que el autor es la persona que está a cargo de la gestión e implementación del proyecto en la compañía CELCO Cía. Ltda.

El proyecto no posee un equipo a cargo del mismo puesto que está conformado solo por el autor que desempeña sus funciones en el área de Sistemas en las oficinas de Quito, con la supervisión del Jefe de Sistemas y Gerencia General que se encuentran en la ciudad de Guayaquil.

Una vez finalizado el proyecto la distribución de los roles se mantiene como se detalló en la factibilidad operacional *Figura 3.7 Organigrama Departamento Sistemas CELCO Cía. Ltda.* mientras que las funciones adicionales que se adquieren al desplegar la herramienta “The Fraud Explorer” se lo detalla en la Tabla 3.2 *Requerimientos mínimos de Recursos Humanos.*

4.1.7 PLANIFICAR LA GESTIÓN DE LOS COSTOS

En la gestión de los costos del proyecto se consideraron las necesidades a nivel de hardware y software a fin de cumplir los requerimientos mínimos necesarios para la implementación de la herramienta de monitoreo y prevención de fraude.

a) ESTIMAR LOS COSTOS

El proyecto no genera ningún costo directo, indirecto o de mano de obra puesto que los equipos informáticos los posee CELCO Cía. Ltda. dentro de su inventario, mientras que los costos de mano de obra se los toma como un costo oculto y representará un valor de cero pues que el proyecto no se realiza dentro del horario laboral.

En el caso de que la organización no posea los equipos necesarios para el despliegue de la herramienta “The Fraud Explorer” se requerirá incurrir en costos de infraestructura y licenciamiento, para mayor detalle revisar Tabla 3.3 *Presupuestos Referenciales.*

4.1.8 ESTIMAR LOS RECURSOS DE LAS ACTIVIDADES

De acuerdo a las actividades establecidas para la gestión e implementación del proyecto el único recurso que está involucrado en todas las actividades es el autor por ser

el líder del proyecto, su perfil está definido en el rol de Gerente del Proyecto e Implementador en la Tabla 3.2 *Requerimientos mínimos de Recursos Humanos*.

4.1.9 ESTIMAR LA DURACIÓN DE LAS ACTIVIDADES

a) DESARROLLAR EL CRONOGRAMA

Para el desarrollo de los cronogramas se consideró el orden de las actividades de implementación que recomienda el fabricante del software The Fraud Explorer además de las etapas de la gestión del proyecto.

En el diseño de los cronogramas se utilizó el Programa Microsoft Project, está basado en el diagrama de Gantt calculando las fechas de inicio y fin de todas las actividades.

Las actividades para la gestión del proyecto, se realizan en simultáneo, con las actividades de implementación, es así que el tiempo total del proyecto está determinado por dichas actividades de implementación. A continuación, se expone el resumen los cronogramas.

A continuación, presentamos el resumen del cronograma con las fechas establecidas para la gestión e implementación de la herramienta “The Fraud Explorer”, para mayor detalle de las actividades revisar Anexo 6. Cronograma de gestión e implementación.

Tabla 4.6 *Cronograma etapas de gestión e implementación*

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Iniciación	5 días	jue 08/11/18	mie 14/11/18	
Planificación	29 días	jue 15/11/18	mar 25/12/18	1
Implementación	15 días	mie 26/12/18	mar 15/01/19	4
Seguimiento y control	18 días	mie 16/01/19	mar 12/02/19	38
Cierre del proyecto	2 días	mie 13/02/19	vie 15/02/19	46

Fuente: Elaboración propia

4.1.10 DETERMINAR EL PRESUPUESTO

En la determinación de la factibilidad económica del proyecto se evaluó 3 escenarios donde se ejemplifica a través de la Tabla 3.3 *Presupuestos Referenciales* si la empresa donde se desea implementar una solución como la que se propone en el presente proyecto no cuenta con los recursos mínimos definidos en la misma deberá incurrir en gastos dependiendo del proveedor el precio puede variar.

CELCO Cía. Ltda. cuenta con el recurso humano e infraestructura para soportar la implementación y despliegue de la herramienta The Fraud Explorer, para mayor detalle revisar Tabla 3.1 *Requerimiento mínimos vs existentes*.

4.1.11 PLANIFICAR LA GESTIÓN DE LA CALIDAD

En la planificación de la calidad presentamos las claves para que la herramienta The Fraud Explorer se mantenga operativa y no presente problemas en su funcionamiento y administración, a continuación, resumimos los factores a tomar en consideración.

Tabla 4.7 Matriz de calidad

Nro.	Objetivo	Actividades	Responsable
1	Mantener el funcionamiento de la herramienta The Fraud Explorer	Mantener operativo el servidor de Directorio Activo	Jefe de Sistemas
		Realizar mantenimiento preventivo a los servidores	Asistente de Sistemas
		Capacitar al personal que administre la herramienta	Gerencia General
2	Reducir los despidos motivados bajo sospechas de fraude	Presentar reportes de detección de posibles fraudes	Asistente de Sistemas
3	Disminuir los casos de fraude	Actualizar las librerías de palabras para la detección y prevención de fraude	Jefe y Asistente de Sistemas

Fuente: Elaboración propia

4.1.12 PLANIFICAR LA GESTIÓN DE LAS COMUNICACIONES

A continuación, detallaremos a través de una matriz RACI como se realizará la gestión de las comunicaciones con los recursos humanos del departamento de sistemas y demás responsables involucrados fin al proyecto.

Tabla 4.8 Matriz RACI Gestión de la comunicación

Nro.	Actividad	Persona y/o Área				
		Diana Fernández	RRHH	Xavier Arroyo	Ronny Plaza	Ronald Coloma
1	Detección de un posible fraude	I	I	A		R
2	Emitir reportes de The Fraud Explorer			A	I	R
3	Agregar y actualizar frase en las librerías del sistema	A	C	A	I	R
4	Reiniciar el servidor The Fraud Explorer	A	I	A	I	R
5	Configurar y Parametrizar The Fraud Explorer	A		A	I	R
6	Monitorear el correcto funcionamiento de la herramienta					R

R: Responsable; A: Autorizado; C: Consultado; I: Informado

Fuente: Elaboración Propia

4.1.13 PLANIFICAR LA GESTIÓN DE LAS ADQUISICIONES

Se realiza la planificación de las adquisiciones, a pesar de que CELCO Cía. Ltda. no va a adquirir nada, pero detallamos las cantidades y descripción de los productos que se necesitarían adquirir en el caso de no poseerlos dentro de su inventario tecnológico.

Tabla 4.9 Detalle de adquisiciones

Ítem	Cantidad	Descripción
1	1	Servidor
2	2	Discos Duros
3	2	Memoria RAM 8GB
4	1	Estación de trabajo
5	1	Licencia The Fraud Explorer
6	1	Licencia Visual Studio 2015
7	1	Licencia Windows Server

Fuente: Elaboración propia

4.1.14 DIRIGIR Y GESTIONAR EL TRABAJO DEL PROYECTO

Las actividades propuestas en la Tabla 4.1 *Actividades de Gestión del Proyecto* y la Tabla 4.2 *Actividades de Implementación* se llevaron a cabo sin cambios por parte de la Gerencia General o Jefe de Sistemas.

4.1.15 GESTIONAR EL CONOCIMIENTO DEL PROYECTO

La implementación de “The Fraud Explorer” en la empresa CELCO Cía. Ltda. genera nuevos conocimientos que contribuirán al aprendizaje de la organización para producir y mejorar los resultados obtenidos con el despliegue de la herramienta antes mencionada, para mayor detalle revisar Anexo 7 Registro de lecciones aprendidas.

4.1.16 GESTIONAR LAS COMUNICACIONES

En el proyecto no se gestiona la comunicación durante el mismo porque no existe un equipo de trabajo, pero se recomienda una vez que se realice el cierre del proyecto se tome como base la matriz de responsabilidades presentada en la Tabla 4.8 *Matriz RACI Gestión de la comunicación* donde se detalla cómo debería fluir las comunicaciones a la interna de la organización con respecto a la herramienta The Fraud Explorer.

4.1.17 GESTIONAR LA CALIDAD

En la gestión de la calidad se recomendó utilizar el círculo de Deming que nos plantea que el éxito de la calidad está en la mejora continua a través del Plan, Do, Check, Act (Costas & Puche, 2010), a continuación, describimos en detalle cómo aplicarlo.

a) PLANIFICAR

Se establece los objetivos que se desea conseguir, para este proyecto nos basaremos en los determinados en la planificación de la calidad.

- Mantener el funcionamiento de la herramienta The Fraud Explorer
- Reducir los despidos motivados bajo sospechas de fraude
- Disminuir los casos de fraude

b) HACER

Se debe implementar y desarrollar las actividades a medida que se deseen cumplir los objetivos planteados.

- Mantener operativo el servidor de Directorio Activo.
- Realizar mantenimiento preventivo a los servidores de AD y The Fraud Explorer.
- Capacitar al personal que administre la herramienta.
- Presentar reportes de detección de posibles fraudes.
- Actualizar las librerías de palabras para la detección y prevención de fraude.

c) VERIFICAR

Se realiza un seguimiento y medición de acuerdo a la actividad realizada para evaluación de los resultados obtenidos.

d) ACTUAR

En esta etapa se enfoca en la toma de decisiones para la mejora y continua, una vez que llegamos a este punto se debe volver a la planificación y así sucesivamente de manera cíclica.

4.1.18 MONITOREAR Y CONTROLAR EL TRABAJO DEL PROYECTO

El control y seguimiento del proyecto se realizó directamente con la Gerencia General manteniendo una comunicación directa a fin de informar el cumplimiento de cada etapa del proyecto tanto en la gestión e implementación.

4.1.19 REALIZAR EL CONTROL INTEGRADO DE CAMBIOS

El presente proyecto no recibió ninguna solicitud de cambio a los entregables, por consecuencia no se tiene documentación que determine la aprobación de los cambios solicitados.

4.1.20 CONTROLAR EL CRONOGRAMA

La planificación del cronograma se ha cumplido de acuerdo al planteado al inicio del proyecto, no fue necesario realizar cambios a la línea base del cronograma.

4.1.21 MONITOREAR LAS COMUNICACIONES

La distribución realizada en la planificación de la gestión de las comunicaciones funciona correctamente de acuerdo a la matriz RACI planteada, su objetivo es generar un diagrama de flujo de comunicación.

4.1.22 MONITOREAR LOS RIESGOS

En la etapa de monitoreo de riesgos se establece un formato para el registro de cada incidente que se pueda presentar posterior a la entrega del proyecto, con el fin de llevar una bitácora con lo sucedido y las acciones que se tomaron de acuerdo a los niveles de riesgo establecidos en la Tabla 4.5 *Categorización de riesgos*, para mayor detalle revisar Anexo 8. Formato de registro incidentes.

4.1.23 CONTROLAR LA CALIDAD

El control de calidad de la herramienta The Fraud Explorer se registró las actividades expuestas en el plan de calidad a fin de validar el correcto funcionamiento y operación de la herramienta desplegada en la infraestructura de la empresa CELCO Cía. Ltda. para que la Gerencia General quede satisfecha. A continuación, se describen las pruebas realizadas y los criterios de aceptación por parte de la Gerencia General.

Tabla 4.10 *Control de calidad*

Ítem	Descripción	Estado	Referencia
1	El servidor AD y The Fraud Explorer se encuentran operativos	Ejecutado	Acta de cierre del proyecto
2	La herramienta detecta un intento de fraude y/u otro acto ilícito	Ejecutado	Acta de cierre del proyecto
3	Las librerías de palabras están relacionadas al giro del negocio	Ejecutado	Acta de cierre del proyecto

4	Existe un plan de mantenimiento de los equipos de computación	Ejecutado	La documentación la tiene el departamento de Sistemas y forma parte de la política del departamento
5	Existe un plan de capacitaciones para el personal	Ejecutado	El plan forma parte de los procesos de apoyo de la organización
6	Posee un plan de comunicación en la detección de un fraude	Ejecutado	Gestión de la comunicación

Fuente: Elaboración propia

4.1.24 CONTROLAR LOS RECURSOS

Los recursos asignados al proyecto no intervienen en el desarrollo del mismo sino cuando este finalice la implementación y gestión, los recursos descritos en la planificación son indispensables para el correcto funcionamiento de la herramienta The Fraud Explorer, se recomienda mantener la estructura propuesta y si es necesario reemplazarlo se lo haga, pero no dejar vacío el rol asignado, para mayor detalle revisar la Tabla 3.2 *Requerimientos mínimos de Recursos Humanos*.

4.1.25 VALIDAR Y CONTROLAR EL ALCANCE

Tabla 4.11 *Validación y control del alcance*

Nro.	Etapas	Actividades	Estado	Observaciones
1	Preparación de hardware y software	Revisar de cumplimiento de requerimientos mínimos	Entregado	Ninguna
		Revisar documentación legal de la herramienta	Entregado	Ninguna
2	Instalación de componentes necesarios en el servidor	Instalación del sistema operativo Centos 7 versión mínima modo texto	Entregado	Ninguna
3	Implementación de la herramienta The Fraud Explorer	Instalar y configurar el servidor The Fraud Explorer	Entregado	Ninguna
4	Parametrización del servidor	Parametrizar de acuerdo al giro del negocio	Entregado	Ninguna
5	Despliegue de los agentes	Parametrizar y configurar el cosechador	Entregado	Ninguna
		Instalar cosechador a través de GPO	Entregado	Ninguna
6	Generación de casos de uso	Generar y detectar casos de fraude	Entregado	Ninguna
		Generar y detectar casos de acoso	Entregado	Ninguna
7	Pruebas	Emitir reportes con los resultados obtenidos	Entregado	Ninguna

Fuente: Elaboración propia

4.1.26 CIERRE DEL PROYECTO

En esta etapa del proyecto se avala el cumplimiento del alcance del proyecto frente a las partes interesadas de la organización, para lo cual se requiere que antes del cierre se realice una aceptación. Lo que significa que ya se debe hacer absolutamente nada más en relación a este proyecto, en caso de existir nuevos requerimientos se deben considerar en un nuevo proyecto, como constancia se adjunta en el Anexo 9. Acta de cierre del proyecto.

4.2 DISEÑO

4.2.1 DESCRIPCIÓN

El servidor The Fraud Explorer está configurado para que recolecte información a través de los agentes desplegados desde el servidor de directorio activo a todos los usuarios, información que pueda derivar en un acto ilícito, su misión es reportar cuando un usuario escriba o confabule en perjuicio de la organización, la herramienta emitirá reportes y alertas, uno de los ejemplos lo vemos a continuación en la *Figura 4.10* Infraestructura de red CELCO Cía. Ltda.

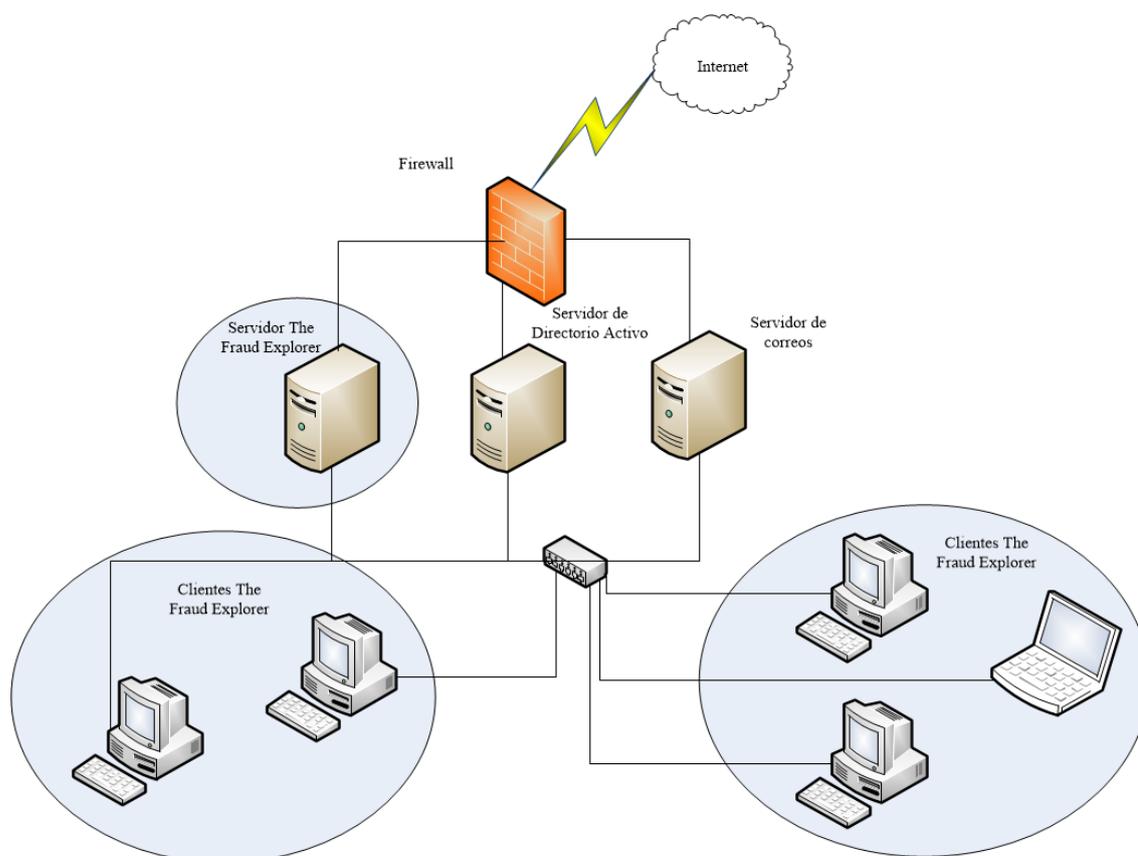


Figura 4.10 Infraestructura de red CELCO Cía. Ltda.
Fuente: Elaboración propia

Los agentes son los encargados de enviar desde los clientes los datos de forma estructurada y encriptada al servidor The Fraud Explorer para su análisis, categorización y alerta en el caso de encontrar coincidencia con las librerías de frases y palabras previamente configuradas, a continuación, se presenta la estructura del archivo xml que envía desde el Endpoint hasta el servidor.

```
<?xml version="1.0"?>
<Domain>
  <User>
    <ID_agt>Identificador del agente</ID_agt>
    <Name>Nombre del usuario</Name>
    <Date>Fecha y hora</Date>
    <Status>0 Offline, 1 Online</Status>
    <AddressIP>Dirección IP del equipo</AddressIP>
    <Rule_Set>Categoría de regla</Rule_Set>
    <Application_Instanse>Nombre de la aplicación</Application_Instanse>
    <Expressing>
      <ph1>Expresión o palabra</ph1>
      <ph2>Expresión o palabra</ph2>
      <ph3>Expresión o palabra</ph3>
    </Expressing>
  </User>
</Domain>
```

4.2.2 IMPLEMENTACIÓN THE FRAUD EXPLORER

Los requisitos preliminares para empezar la implementación de la herramienta The Fraud Explorer los detallamos a continuación.

- 1) Instalar Visual Studio Profesional 2017 en un equipo con sistema operativo Windows 10 Pro 64 bits.
- 2) Implementar y configurar un servidor de Active Directory con Microsoft Windows Server 2003 en adelante, 32bit o 64bit. Esto es opcional puesto que se puede desplegar el instalador de manera manual.
- 3) Servidor The Fraud Explorer con los siguientes componentes: Apache web Server con módulo mod_rewrite, PHP 5.6.30, Open SSL, Motor de base de datos MariaDB y Grupo de herramientas de desarrollo "Development Tools".

El primer paso es configurar los clientes, descargar y configurar el archivo Settings.cs en el código ubicar mainServer y colocar la dirección https completa del servidor terminada en el recurso update.xml y analyticsServer agregar la dirección IP completa del servidor, después se compilan los archivos.

El link de descarga de los archivos es el siguiente:

<https://github.com/nfsecurity/the-fraud-explorer/tree/master/Behavioral%20Harvester>

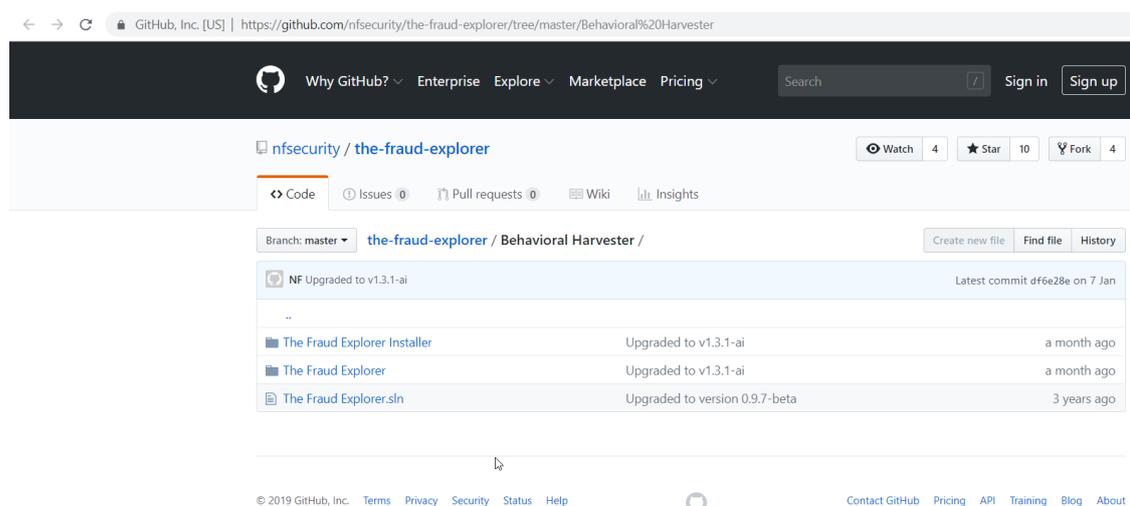


Figura 4.11 Ubicación archivos fuente
Fuente: (NFC Security, 2018)

El archivo MSI generado se debe desplegar en los equipos de la empresa. Existen dos formas de instalar el MSI, a través de un controlador de dominio con políticas de grupo (GPO) o de forma individual, instalando PC por PC el MSI.

La instalación mediante GPO se realiza ubicando el archivo thefraudexplorer.msi en una ruta alcanzable por todos los usuarios registrados en el Directorio Activo, a continuación, detallamos los pasos a seguir.

- Abrir el Administración de Políticas de Grupo en el menú Iniciar herramientas administrativas Administración de políticas de grupo.
- Seleccionar el bosque por defecto dominio por defecto Objetos de directiva de grupo, luego dar clic derecho en él y luego en nuevo.
- Escoger un nombre de política, es recomendable para esta solución usar uno como Fraud Triangle Analytics
- En mostrar enlaces en esta ubicación seleccionar el bosque por defecto.
- Asegurarse de que en el campo Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO contenga la lista de unidades organizacionales a las que se les aplicará globalmente la GPO. Esto no significa que aquí se desplegará, sino que se utilizará como base para el filtro del siguiente paso.

- En Filtrado de seguridad se deben agregar los usuarios del dominio a los cuales se les desplegará el software.
- Dar clic en el OU al cual pertenece el usuario a asignar el software y hacer link de la política dando clic derecho en el OU y luego en Vincular un GPO existente, para posteriormente seleccionar Fraud Triangle Analytics Software.
- Dar clic en Objetos de directiva de grupo y luego clic derecho en la política Fraud Triangle Analytics y seleccionar Editar
- En Políticas de configuración de usuario dar clic en Configuración de Software, luego en Instalación de Software, dar clic en Nuevo Paquete.
- Seleccionar el archivo msrhl64svc.msi en la ruta de red compartida creada en el procedimiento de ubicación del agente.
- Seleccionar Avanzado en la lista de opciones de despliegue.
- Seleccionar la pestaña Despliegue, luego dar clic en la opción Asignado, luego en Desinstale esta aplicación cuando esté fuera del alcance de la administración y luego en Instale esta aplicación en el inicio de sesión.
- Presionar el botón OK.

Configurar el servidor basado en Linux se recomienda utilizar Centos o Redhat 7 64 bits, a continuación, se detallan los pasos para su configuración a partir de la instalación del sistema operativo versión mínima modo texto.

- Instalar el repositorio EPEL

```
# rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```
- Deshabilitar SELinux en el archivo `/etc/sysconfig/selinux` con `SELinux=disabled`

```
# setenforce 0; reboot
```
- Instalar las herramientas de desarrollo

```
# yum groupinstall "Development Tools"
# yum install yasm pkgconfig libXext-devel libXfixes-devel zlib-devel
```
- Ajustar el archivo `/etc/hosts`

```
192.168.10.10 myhostname.mydomain.com
```
- Servidor de correo Postfix

```
# yum install postfix
```

```
# mkdir /etc/postfix/private ; cd /etc/postfix/private
# echo "[smtp.mysmtpserver.com] smtp@mysmtpserver.com:my password" >
saspasswd
# postmap canonical ; postmap saspasswd ; postmap sender_relay
```

- Agregar este segmento de líneas en el archivo main.cf

```
relayhost =
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/private/saspasswd
smtp_sasl_security_options = noanonymous
smtp_sasl_type = cyrus
smtp_sasl_mechanism_filter = login
smtp_sender_dependent_authentication = yes
```

- Ajustar las líneas myorigin y mydomain en el archivo main.cf. Asegúrese de que el hostname se resuelva a través de los DNS.

```
# yum install epel-release
# rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
# yum --enablerepo=remi-php73 install php
# yum install httpd
# yum --enablerepo=remi-php73 install php-xml php-soap php-xmlrpc php-
mbstring
# yum --enablerepo=remi-php73 install php-json php-gd php-mcrypt php-zip
# yum --enablerepo=remi-php73 install php73-php-pspell php73-php-json php-
mysqlnd
# yum install mod_ssl libmcrypt-devel libmcrypt
```

- Compilar Ruby y RubyGems

```
# yum install -y git-core zlib zlib-devel gcc-c++ patch readline readline-devel
# yum install libyaml-devel openssl-devel make bzip2 autoconf automake libtool
```

```
# yum install bison curl sqlite-devel

# cd; git clone git://github.com/sstephenson/rbenv.git .rbenv

# echo 'export PATH="$HOME/.rbenv/bin:$PATH"' >> ~/.bash_profile

# echo 'eval "$(rbenv init -)"' >> ~/.bash_profile

# exec $SHELL

# git clone git://github.com/sstephenson/ruby-build.git ~/.rbenv/plugins/ruby-build

# echo 'export PATH="$HOME/.rbenv/plugins/ruby-build/bin:$PATH"' >>
~/.bash_profile

# exec $SHELL

# .rbenv/bin/rbenv install -v 2.3.0

# .rbenv/bin/rbenv global 2.3.0
```

- Salir del shell, ingresar nuevamente y ejecutar el siguiente comando:

```
# gem install bundler ruby-mcrypt openssl base bundle rubysl-base64
```

- Eliminar los archivos innecesarios

```
# rm /etc/httpd/conf.d/welcome.conf
```

- Configurar los Virtual Hosts en Apache en el archivo /etc/httpd/conf.d/ssl.conf:

```
Listen 443 https
```

```
SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog
```

```
SSLSessionCache shmcb:/run/httpd/sslcachel(512000)
```

```
SSLSessionCacheTimeout 300
```

```
SSLRandomSeed startup file:/dev/urandom 256
```

```
SSLRandomSeed connect builtin
```

```
SSLCryptoDevice builtin
```

```
<VirtualHost _default_:443>
```

```
    DocumentRoot "/var/www/html/thefraudexplorer"
```

```
    ServerName console.mydomain.com:443
```

```
ErrorLog logs/mydomain-error_log
TransferLog logs/mydomain-access_log
LogLevel warn
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256
SSLCertificateFile /etc/letsencrypt/live/console.mydomain.com/cert.pem
SSLCertificateKeyFile
/etc/letsencrypt/live/console.mydomain.com/privkey.pem
<Files ~ "\.(cgi|shtml|phtml|php3?)$" >
    SSLOptions +StdEnvVars
</Files>
<Directory /var/www/html/thefraudexplorer/rest>
<Limit GET POST DELETE PUT OPTIONS>
    Require all granted
</Limit>
<LimitExcept GET POST DELETE PUT OPTIONS>
    Require all denied
</LimitExcept>
</Directory>
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
BrowserMatch "MSIE [2-5]" \
```

```

    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
    CustomLog logs/mydomain-request_log \
        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
    AllowEncodedSlashes On
    RewriteEngine on
    RewriteCond %{THE_REQUEST} !^(POST|GET|PUT|DELETE)\ /.*\
    HTTP/1\..1$
    RewriteRule .* - [F]
    SSLCertificateChainFile
    /etc/letsencrypt/live/console.mydomain.com/chain.pem
</VirtualHost>

```

- Crear los certificados digitales a usar con Let's Encrypt:

```

# yum install httpd mod_ssl python-certbot-apache
# certbot --apache -d console.mydomain.com

```

Cambiar las directivas `ServerName`, `SSLCertificateFile`, `SSLCertificateKeyFile`, `SSLCertificateChainFile`, `ErrorLog`, `CustomLog` y `DocumentRoot` como corresponda.

- En el archivo de configuración `/etc/httpd/conf/httpd.conf` modificar:

```

<Directory "/var/www/html">
    AllowOverride None

```

- Por lo siguiente, para activar el `mod_rewrite`:

```

<Directory "/var/www/html">
    AllowOverride All

```

- Y agregar al final:

```

Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
Header always append X-Frame-Options SAMEORIGIN

```

```
<Directory /var/www/html/thefraudexplorer>
```

```
Options -Indexes
```

```
</Directory>
```

- Ajustar los parámetros del archivo php.ini:

```
max_execution_time = 1300
```

```
max_input_time = 1600
```

```
memory_limit = 1024M
```

```
display_errors = On
```

```
post_max_size = 500M
```

```
upload_max_filesize = 500M
```

```
date.timezone = America/Bogota
```

Motor de base de datos

- Agregar el siguiente repositorio para MariaDB en el archivo /etc/yum.repos.d/MariaDB.repo:

```
[mariadb]
```

```
name = MariaDB
```

```
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
```

```
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
```

```
gpgcheck=1
```

- Configurar la base de datos e importe la estructura inicial de The Fraud Explorer

```
# yum install mariadb-server MariaDB-client mariadb-libs mariadb
```

```
# systemctl start mariadb
```

```
# mkdir /var/www/html/thefraudexplorer
```

```
# mkdir /home/thefraudexplorer ; cd /home/thefraudexplorer
```

```
# git clone https://github.com/nfsecurity/the-fraud-explorer.git
```

```
# cd the-fraud-explorer/Application\ Dashboard/
```

```
# mv thefraudexplorer/* /var/www/html/thefraudexplorer/
```

```
# cd /var/www/html/thefraudexplorer
```

```
# mysql -u root -p
```

➤ MariaDB> create database thefraudexplorer;

```
MariaDB> GRANT ALL ON thefraudexplorer.* TO 'tfe'@'localhost'  
IDENTIFIED BY 'mypass';
```

```
MariaDB> flush privileges;
```

```
MariaDB> exit;
```

```
# mysql -u root -p thefraudexplorer < sqlcsv/thefraudexplorer.sql
```

En la tabla `t_users` ya se encuentra el usuario `admin`, con el que más adelante se iniciará sesión en la plataforma web de administración. Este usuario tiene la contraseña por defecto `N0FR4UD`.

- Configurar en el archivo `/var/www/html/thefraudexplorer/config.ini` el usuario y contraseña que configuró para el acceso a la base de datos `thefraudexplorer`
- Ajustar la configuración en el archivo `/etc/my.cnf` así, para una máquina con 32 GB de RAM:

```
[mysqld]
```

```
key_buffer_size = 1024M
```

```
max_allowed_packet = 64M
```

```
wait_timeout = 300
```

```
max_connections = 1024
```

```
innodb_flush_method = O_DIRECT
```

```
innodb_buffer_pool_size = 1024M
```

```
thread_cache_size = 8
```

```
query_cache_size = 64M
```

```
query_cache_limit = 4M
```

```
table_cache = 35000
```

```
table_open_cache = 35000
table_definition_cache = 10400
open_files_limit = 65000
innodb_file_per_table
sort_buffer_size = 32M
sql_mode = ""
```

- Instalar ASPELL y el diccionario en español usado por The Fraud Explorer

```
# yum install aspell aspell-devel
# cd /home/thefraudexplorer
# yum install wget -y
# wget ftp://ftp.gnu.org/gnu/aspell/dict/es/aspell6-es-1.11-2.tar.bz2
# bunzip2 aspell6-es-1.11-2.tar.bz2 ; tar xvf aspell6-es-1.11-2.tar
# cd aspell6-es-1.11-2 ; ./configure ; make ; make install
```

- Ajustar la configuración global

Edite el archivo `/var/www/html/thefraudexplorer/config.ini` y ajuste las variables.

```
[php]
php_timezone = "America/Bogota"
php_server_url = "https://console.mydomain.com"
php_document_root = "/var/www/html/thefraudexplorer/"
```

Correo electrónico

- Configurar Postfix para el envío de correos electrónicos a través de su servidor de correo. The Fraud Explorer envía un correo cada vez que un agente genera una alerta a través del sistema de inteligencia artificial.
- Configurar en el archivo `/var/www/html/thefraudexplorer/config.ini` sus opciones de correo electrónico:

```
[mail]
mail_to = "smtp@mydomain.com"
```

```
mail_subject = "[The Fraud Explorer] Fraud Triangle Alert From: "
```

```
mail_from = "From: smtp@mydomain.com"
```

```
mail_reply_to = "Reply-To: smtp@mydomain.com"
```

- Configurar e instalar el software Curator que servirá para realizar mantenimiento a los índices donde se almacenan las alertas y las palabras, a través del módulo Maintenance de The Fraud Explorer, a continuación, detallamos los comandos a ejecutar:

```
# yum install python python-devel python-pip
```

```
# pip install --upgrade pip
```

```
# pip install elasticsearch-curator
```

- Al terminar, copiar el archivo curator creado a la ruta /lbs/curator/bin del directorio principal de The Fraud Explorer para re-emplazar la versión proporcionada en este paquete, en caso de que esté mas desactualizada.
- Para permitir la ejecución de este script de mantenimiento, agregar al archivo SUDOERS de Linux los permisos necesarios para su ejecución:

```
# visudo
```

```
apache ALL=NOPASSWD: /usr/bin/python
```

- Para que funcione la descarga de reglas cuando se da clic en Download rules es necesario crear el directorio vacío en el core del procesador de reglas así:

```
# cd /var/www/html/thefraudexplorer/core
```

```
# mkdir ziprules
```

- Instalar Java 8 de Oracle:

```
# cd ~
```

```
# wget --no-cookies --no-check-certificate \
```

```
--header "Cookie: gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; \
```

```
oraclelicense=accept-securebackup-cookie" \
```

```
"http://download.oracle.com/otn-pub/java/jdk/8u192-
```

```
b12/750e1c8617c5452694857ad95c3ee230/jre-8u192-linux-x64.rpm"
```

```
# yum -y localinstall jre-8u192-linux-x64.rpm
```

- Instalar la llave GPG de Elasticsearch:

```
# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

- Configurar el repositorio de Elasticsearch:

```
# echo '[elasticsearch-6.x]
```

```
name=Elasticsearch repository for 6.x packages
```

```
baseurl=https://artifacts.elastic.co/packages/6.x/yum
```

```
gpgcheck=1
```

```
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

```
enabled=1
```

```
' | sudo tee /etc/yum.repos.d/elasticsearch.repo
```

- Instalar Elasticsearch con el comando:

```
# yum -y install elasticsearch
```

- Editar el archivo de configuración de Elasticsearch y establezca la propiedad `network.host` a `localhost`:

```
# vim /etc/elasticsearch/elasticsearch.yml
```

```
# systemctl start elasticsearch
```

- En ese mismo archivo de configuración `elasticsearch.yml` agregar lo siguiente al final:

```
indices.requests.cache.size: 10%
```

```
indices.queries.cache.size: 20%
```

```
thread_pool.bulk.queue_size: 10240
```

```
thread_pool.search.queue_size: 10240
```

- Instalar Logstash:

```
# yum -y install logstash
```

- Verificar que JRuby posee la gema `jruby-openssl` e instale otras gemas. Asegúrese de que las gemas quedan instaladas en el directorio `/usr/share/logstash/vendor/bundle/jruby/2.3.0`:

```
# env GEM_HOME=/usr/share/logstash/vendor/bundle/jruby/2.3.0
#/usr/share/logstash/vendor/jruby/bin/jruby
/usr/share/logstash/vendor/jruby/bin/gem list
#/usr/share/logstash/vendor/jruby/bin/jruby
/usr/share/logstash/vendor/jruby/bin/gem install rubysl-base64 jdbc-mysql inifile
```

- Añadir al archivo `/usr/share/logstash/Gemfile` lo siguiente:

```
gem "inifile"
gem "jdbc-mysql"
gem "rubysl-base64"
```

- Para luego ejecutar el comando:

```
# /usr/share/logstash/bin/logstash-plugin update logstash-filter-grok
```

- Descargar el conector Java de MySQL para Logstash:

```
# cd /opt
# wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-5.1.47.zip
# unzip mysql-connector-java-5.1.47.zip
# rm mysql-connector-java-5.1.47.zip
```

- Crear el archivo de configuración `/etc/sysconfig/logstash` y agregue la línea:

```
CLASSPATH=/opt/mysql-connector-java-5.1.47/mysql-connector-java-5.1.47-
bin.jar:$CLASSPATH
```

- Copiar el JAR del driver de MySQL a la ruta donde Logstash almacena los JAR:

```
# cp mysql-connector-java-5.1.47-bin.jar /usr/share/logstash/logstash-core/lib/jars/
```

- Configurar Logstash para recibir los datos de The Fraud Explorer en el directorio `/etc/logstash/conf.d`. Copie el contenido del directorio `conf.d` a su ubicación local.

- Establecer los parámetros de memoria para Logstash en `/etc/logstash/jvm.options`:

-Xms3g

-Xmx3g

➤ Iniciar Logstash:

```
# systemctl start logstash
```

Una vez que finalizamos los pasos abrimos el navegador Google Chrome porque es el único diseñado para soportar la interfaz de la herramienta de monitoreo y administración The Fraud Explorer, el url de acceso es el dominio creado o la dirección IP asignada al servidor en la configuración mínima del servidor Centos 7 modo texto.

4.2.3 OPERACIÓN THE FRAUD EXPLORER

The Fraud Explorer se puede acceder a través de la web una vez que se inicie sesión con las credenciales respectivas con lo vemos en la *Figura 4.12*.

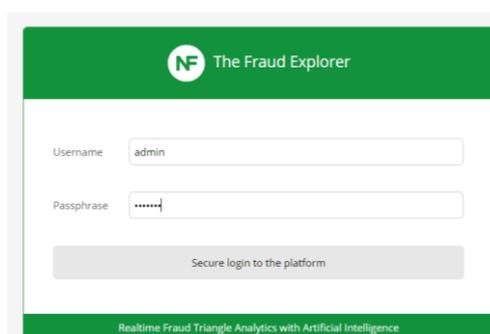


Figura 4.12 Login The Fraud Explorer
Fuente: Elaboración propia

Una vez que iniciamos sesión visualizaremos 4 ventanas, una muestra los primeros 50 equipos registrados ordenándolos por la puntuación que se ha sumado a través del tiempo basándose en el triángulo del fraude. Otra ventana muestra las estadísticas referente a todos los equipos conectados y registrados en la herramienta. Otra ventana muestra el puntaje total de la compañía en relación al fraude, organizándolo por la cantidad de ocurrencias que haya tenido dependiendo de las categorías: Presión, Oportunidad y Justificación. La última ventana indica las últimas 50 alertas emitidas discriminándolo por equipo, palabra o frase escrita y la aplicación utilizada.

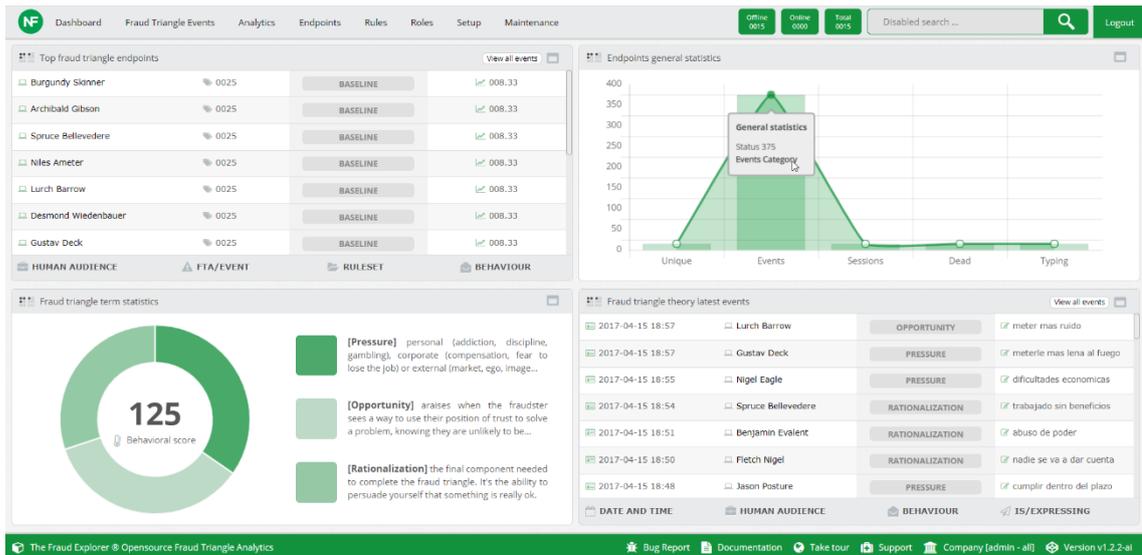


Figura 4.13 Ventana principal
Fuente: Elaboración propia

En el menú principal disponemos de la opción Endpoints donde se despliega a modo de listado todos los usuarios que están registrados, además se tiene a disposición su identificación, sexo, fecha de última conexión.

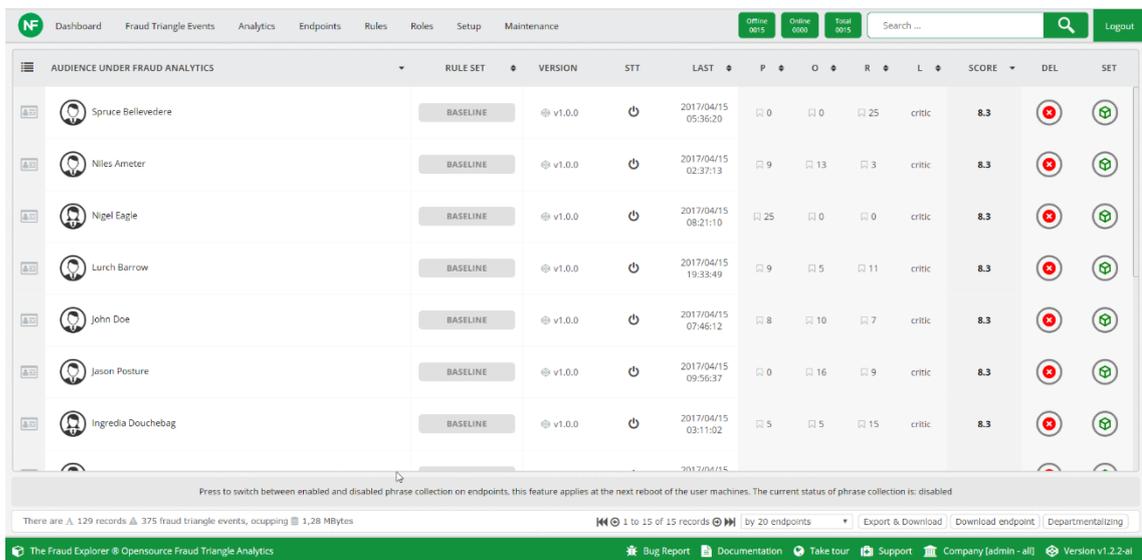


Figura 4.14 Ventana Endpoints
Fuente: Elaboración propia

En la opción Analytics se observa en forma de puntos los usuarios que han generado alertas. Cada uno de los puntos se los puede dar un clic su detalle.

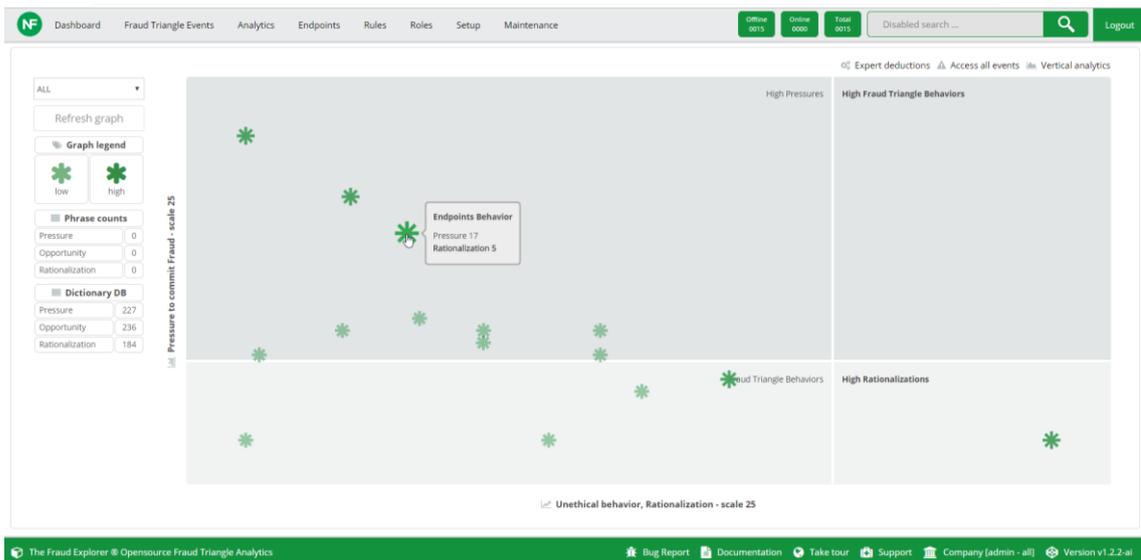


Figura 4.15 Ventana analytics
Fuente: Elaboración propia

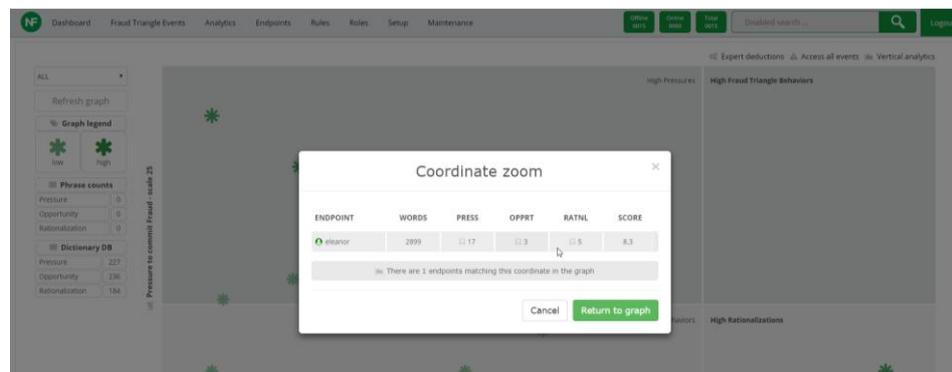


Figura 4.16 Detalle Analytics
Fuente: Elaboración propia

En cualquier momento podemos dar un clic en un usuario ya sea en la ventana principal o en la opción Analytics se podrá observar todas las alertas emitidas por dicho usuario.

DATE	BEHAVIOUR	APPLICATION INSTANCE	IS/EXPRESSION	MARK
2017-04-15 21:52	PRESSURE	Microsoft Word - Listado de proveedores ultimo semestre.docx	<input type="checkbox"/> cumplir dentro del plazo	<input checked="" type="checkbox"/>
2017-04-15 20:45	OPPORTUNITY	Skype Business - Conversacion con Noel Medina	<input type="checkbox"/> que parezcan errores	<input checked="" type="checkbox"/>
2017-04-15 20:38	OPPORTUNITY	Google Search - Como borrar archivos definitivamente	<input type="checkbox"/> desaparecan los documentos	<input checked="" type="checkbox"/>
2017-04-15 20:27	PRESSURE	Google Search - Como hackear un correo electronico	<input type="checkbox"/> me tienen chuzado	<input checked="" type="checkbox"/>
2017-04-15 20:23	PRESSURE	Skype Business - Conversacion con Luis Salazar	<input type="checkbox"/> dificultades economicas	<input checked="" type="checkbox"/>
2017-04-15 19:41	RATIONALIZATION	Gmail Inbox - Bandeja de correo no deseado	<input type="checkbox"/> poco eticos	<input checked="" type="checkbox"/>
2017-04-15 19:29	PRESSURE	Gmail Inbox - Bandeja de correo no deseado	<input type="checkbox"/> evadir la auditoria	<input checked="" type="checkbox"/>
2017-04-15 19:27	RATIONALIZATION	Google Search - Como hackear un correo electronico	<input type="checkbox"/> abuso de poder	<input checked="" type="checkbox"/>
2017-04-15 18:52	RATIONALIZATION	Google Search - Como desprestigiar a mi jefe	<input type="checkbox"/> hay que avisarse	<input checked="" type="checkbox"/>
2017-04-15 18:51	PRESSURE	Skype Business - Chat con Julio Andres Monsalve	<input type="checkbox"/> vigilan el tiempo	<input checked="" type="checkbox"/>

Figura 4.17 Detalle alertas
Fuente: Elaboración propia

4.2.4 ADMINISTRACIÓN THE FRAUD EXPLORER

La herramienta The Fraud Explorer tiene más ventanas dedicadas a la configuración, a continuación las detallamos.

En la opción rules se puede descargar o actualizar el diccionario de palabras que se encuentra configurado, categorizado por la presión, oportunidad y racionalización.

RULESET	PRESS	OPPR	RATNL	TOTAL	ENDPT
HUMAN	10	11	11	32	0
FINANCE	35	55	31	121	0
LEGAL	10	10	10	30	0
SALES	20	21	19	60	0
AUDIT	10	11	10	31	0
LOGISTIC	10	14	10	34	0
CUSTOMER	10	13	10	33	0
TAXES	15	8	8	31	0
PROJECTS	10	8	6	24	0
OPERATIONS	0	0	0	0	0

Figura 4.18 Configuración reglas
Fuente: Elaboración propia

En la opción de Setup se desplegará la configuración principal de la herramienta, también permite: Activar o desactivar el cálculo de datos que por defecto viene cargado en la solución, cambiar la contraseña de conexión de los usuarios al servidor, cambiar la

clave de administración y por ultimo nos permite configurar el puntaje que se asigna a cada usuario.

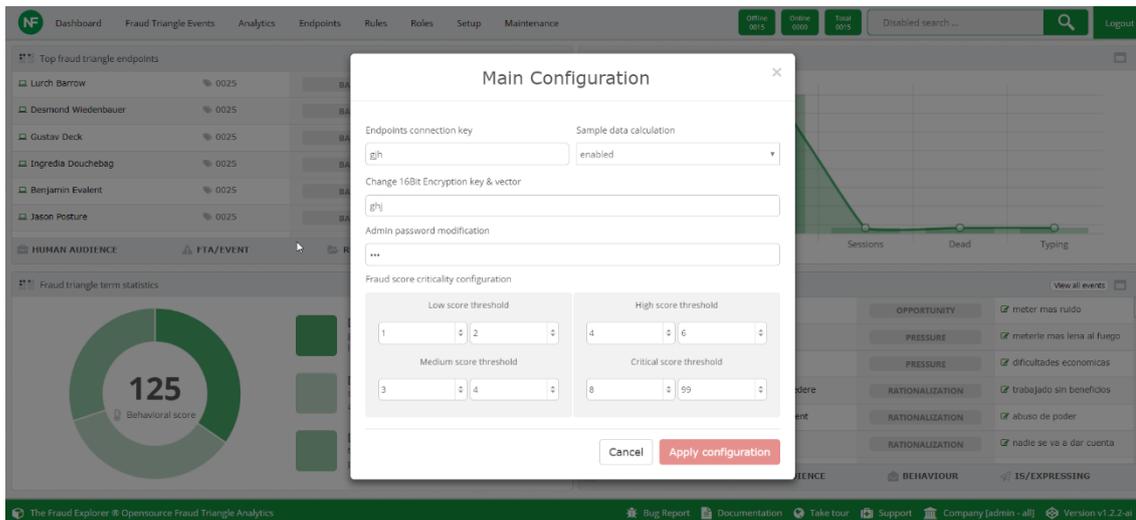


Figura 4.19 Configuración principal
Fuente: Elaboración propia

En la opción de Roles se abrirá una ventana que nos permite agregar, editar o eliminar usuarios.

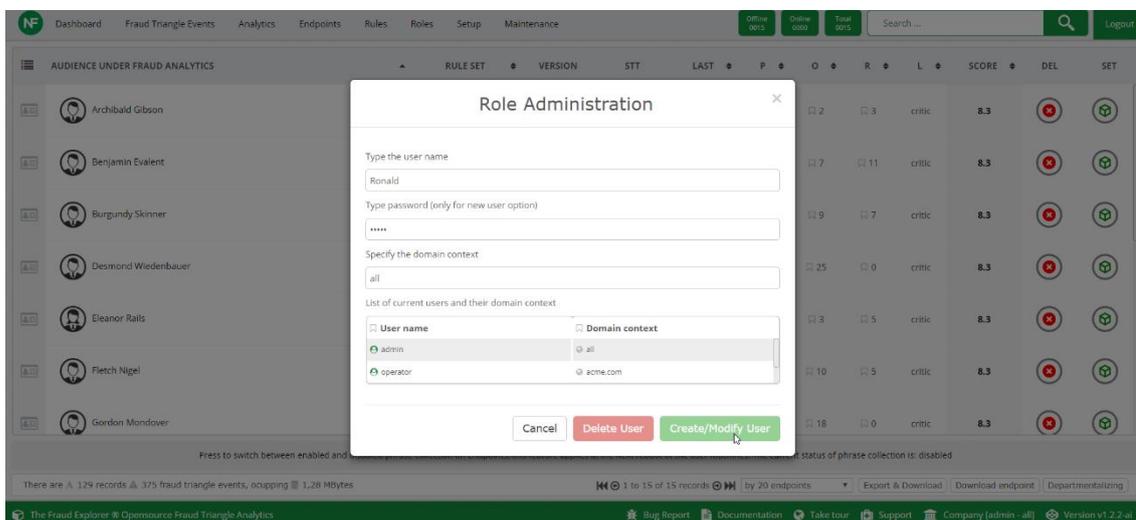


Figura 4.20 Administración de roles
Fuente: Elaboración propia

La herramienta nos da una opción de Maintenance que permite realizar el mantenimiento del Elasticsearch y de la base de datos sobre todo cuando presentamos problemas de almacenamiento esto se produce por la cantidad de datos.

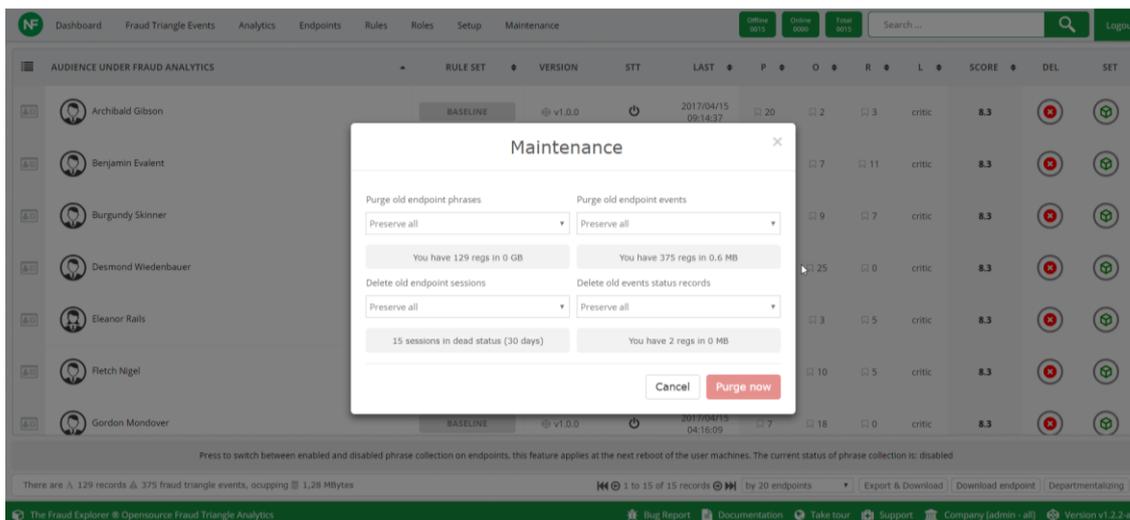


Figura 4.21 Mantenimiento
Fuente: Elaboración propia

4.2.5 RESULTADOS

Para la demostración de resultados se basó en el modelo experimental que se representa “como el procedimiento de planeación y conducción de experimentos, así como la definición del análisis estadístico para evaluar los resultados, con el objetivo de tener conclusiones válidas y objetivas” (Mellado, 2015).

A continuación, describimos cada una de las etapas del modelo de diseño experimental que se utilizó para comprobar el funcionamiento de la herramienta The Fraud Explorer.

a) DATOS DE ENTRADA

Tabla 4.12 Datos de entrada

Usuario	Fecha	Categorización	Aplicación	Palabra / Frase
Karla Riera	14/02/2019	Presión	Google	Crisis en la empresa
			Skype	Están vigilando
			Microsoft Word	Usted nunca supo nada
			Yahoo	Como desprestigiar a mi jefe
Víctor Borja	14/02/2019	Racionalización	Skype	Vacaciones costosas
		Racionalización	Notepad	Ellos también roban
			Power Point	Deseo un sueldo alto
			Whatsapp Web	Cuánto vale tu silencio
		Presión	Skype	Dificultades económicas

Fuente: Elaboración propia

b) PROCESO

A continuación, presentamos a través de un diagrama de flujo los múltiples procesos que realiza el agente y el servidor partiendo desde la entrada de datos hasta la representación de los resultados.

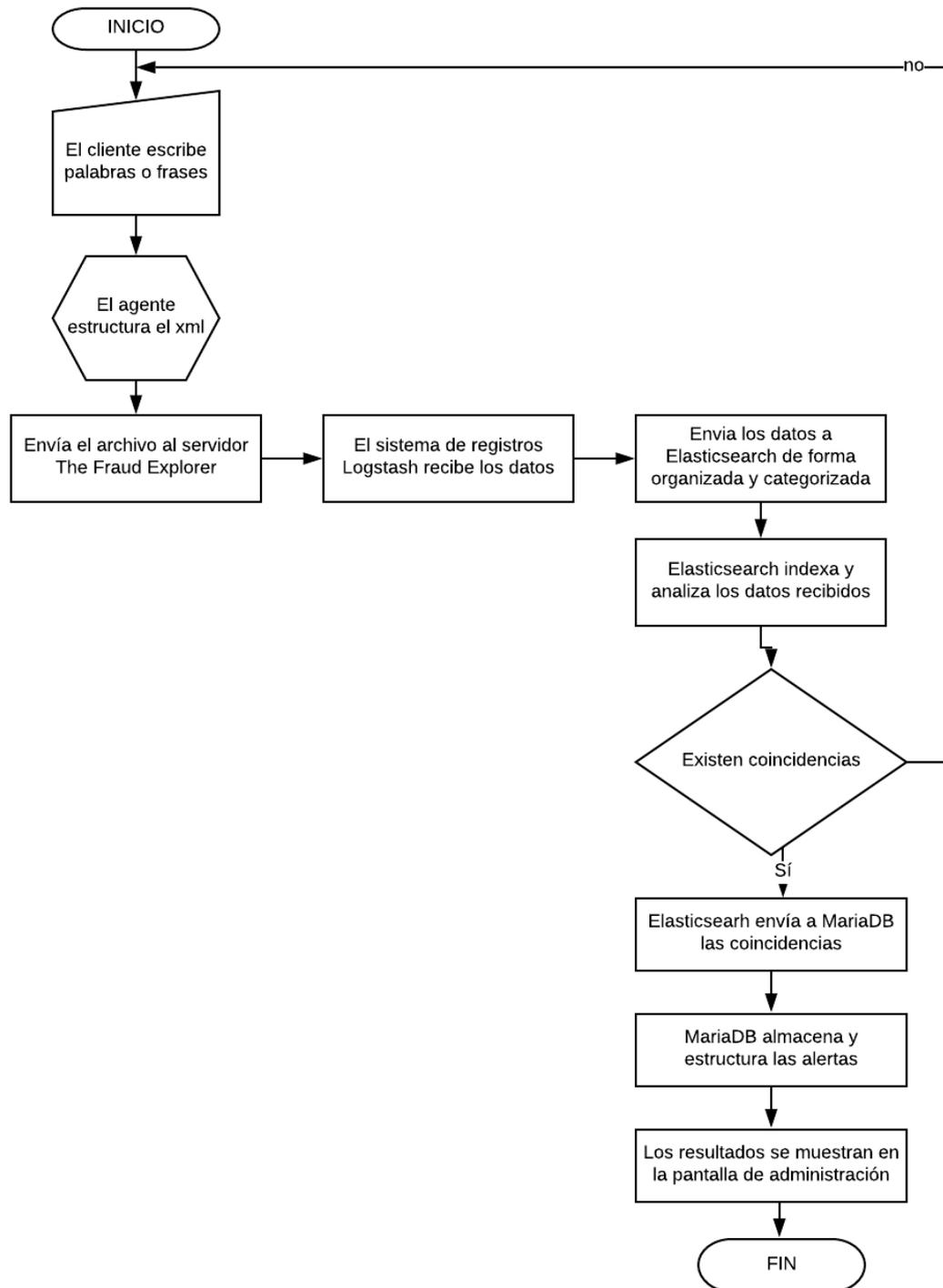


Figura 22 Diagrama de proceso The Fraud Explorer
Fuente: Elaboración propia

c) RESULTADO ESPERADO

Una vez finalizado el proceso de las frases y palabras ingresadas su resultado es satisfactorio puesto que la herramienta demuestra que es capaz de identificar a los usuarios que intenten realizar fraude o inciten a cometer delitos en perjuicio de la empresa. Para demostrar los resultados obtenidos de estas simulaciones se presentan las siguientes figuras.

DATE	BEHAVIOUR	APPLICATION INSTANCE	IS/EXPRESSIONING	MARK
2019-02-14 16:14	PRESSURE	Google Search - Represion en el trabajo	crisis en la empresa	✓
2019-02-14 15:42	PRESSURE	Skype	vigilan el tiempo	✓
2019-02-14 15:25	PRESSURE	Microsoft Word - Listado de proveedores ultimo semestre.docx	cumplir dentro del plazo	✓
2019-02-14 13:24	PRESSURE	Google Search - Como desprestigiar a mi jefe	estoy bajo mucha presion	✓
2019-02-14 12:47	PRESSURE	Microsoft Word - Documento de comunicacion personal.docx	usted nunca supo nada	✓
2019-02-14 11:52	PRESSURE	Yahoo Preguntas - Mi jefe el sapo	maneje la situacion con mucha...	✓
2019-02-14 11:44	PRESSURE	Google Search - Como borrar archivos definitivamente	mi situacion es critica	✓
2019-02-14 11:40	PRESSURE	Microsoft Project - Cronograma ajustado proyecto Azul.mpp	están espiando	✓
2019-02-14 11:31	PRESSURE	Microsoft Project - Proyecto construccion casa.mpp	dejese querer	✓
2019-02-14 11:27	PRESSURE	Microsoft Excel - Resumen de finanzas personales.xlsx	problemas con la familia	✓

Figura 4.23 Resultados simulación 1

Fuente: (CELCO Cía. Ltda., 2019)

Elaborado por el autor

DATE	BEHAVIOUR	APPLICATION INSTANCE	IS/EXPRESSIONING	MARK
2019-02-14 18:58	PRESSURE	Skype	vacaciones muy costosas	✓
2019-02-14 18:56	RATIONALIZATION	Microsoft PowerPoint - Presentacion estado del proyecto SAP.pptx	ellos tambien roban	✓
2019-02-14 18:52	RATIONALIZATION	Notepad - Carta salario.docx	deseo un sueldo alto	✓
2019-02-14 18:47	PRESSURE	WhatsApp Web	usted no sabe nada	✓
2019-02-14 17:45	PRESSURE	Google Search - Como borrar archivos definitivamente	mi situacion es critica	✓
2019-02-14 17:42	RATIONALIZATION	Microsoft PowerPoint - Presentación junta directiva.pptx	mezco mucho mas	✓
2019-02-14 15:41	PRESSURE	Google Search - Como ganar mas dinero facil y rapido	lo necesito como sea	✓
2019-02-14 15:36	PRESSURE	SAP GUI - Transaccion extranjera	manejas la situacion con cuida...	✓
2019-02-14 15:22	PRESSURE	Skype	cuanto vale su silencio	✓
2019-02-14 14:44	PRESSURE	Skype	dificultades economicas	✓

Figura 4.24 Resultados simulación 2

Fuente: (CELCO Cía. Ltda., 2019)

Elaborado por el autor

4.2.6 PRUEBAS REALIZADAS

En la primera simulación realizada se tomó como referencia a la Ing. Karla Riera del departamento comercial actualmente en el cargo de Asistente de ventas y desde su computador el día 14 de febrero de 2019 se ingresó a varias aplicaciones ingresando múltiples frases como se detalla en la Tabla 4.13 *Simulación 1 Karla Riera*. Los resultados arrojados por la herramienta son del agrado de la Gerencia General puesto que la herramienta detecta y categoriza de acuerdo a Usuario, fecha, aplicación y frases detectadas para mayor detalle revisar *Figura 4.25 Simulación Karla Riera*.

Tabla 4.13 Simulación 1 Karla Riera

Usuario	Fecha	Categorización	Aplicación	Palabra / Frase
Karla Riera	14/02/2019	Presión	Google	Crisis en la empresa
			Skype	Están vigilando
			Microsoft Word	Usted nunca supo nada
			Yahoo	Como desprestigiar a mi jefe

Fuente: Elaboración propia

DATE	BEHAVIOUR	APPLICATION INSTANCE	IS/EXPRESSIONS	MARK
2019-02-14 16:14	PRESSURE	Google Search - Represion en el trabajo	crisis en la empresa	✓
2019-02-14 15:42	PRESSURE	Skype	vigilan el tiempo	✓
2019-02-14 15:25	PRESSURE	Microsoft Word - Listado de proveedores ultimo semestre.docx	cumplir dentro del plazo	✓
2019-02-14 13:24	PRESSURE	Google Search - Como desprestigiar a mi jefe	estoy bajo mucha presion	✓
2019-02-14 12:47	PRESSURE	Microsoft Word - Documento de comunicacion personal.docx	usted nunca supo nada	✓
2019-02-14 11:52	PRESSURE	Yahoo Preguntas - Mi jefe el sapo	maneje la situacion con mucha...	✓
2019-02-14 11:44	PRESSURE	Google Search - Como borrar archivos definitivamente	mi situacion es critica	✓
2019-02-14 11:40	PRESSURE	Microsoft Project - Cronograma ajustado proyecto Azul.mpp	están espiondo	✓
2019-02-14 11:31	PRESSURE	Microsoft Project - Proyecto construccion casa.mpp	dejesse querer	✓
2019-02-14 11:27	PRESSURE	Microsoft Excel - Resumen de finanzas personales.xlsx	problemas con la familia	✓

Figura 4.25 Simulación Karla Riera

Fuente: (CELCO Cía. Ltda., 2019)

Elaborado por el autor

Para la segunda simulación realizada se tomó como referencia al Sr. Víctor Borja del departamento financiero actualmente en el cargo de Contador General y desde su computador el día 14 de febrero de 2019 se ingresó a varias aplicaciones ingresando múltiples frases como se detalla en la Tabla 4.14 *Simulación 1 Víctor Borja*. Los resultados arrojados por la herramienta son del agrado de la Gerencia General puesto que

la herramienta detecta y categoriza de acuerdo a Usuario, fecha, aplicación y frases detectadas para mayor detalle revisar *Figura 4.26 Simulación Víctor Borja*.

Tabla 4.14 Simulación 2 Víctor Borja

Usuario	Fecha	Categorización	Aplicación	Palabra / Frase
Víctor Borja	14/02/2019	Presión	Skype	Vacaciones costosas
		Racionalización	Notepad	Ellos también roban
		Racionalización	Power Point	Deseo un sueldo alto
		Presión	Whatsapp Web	Cuánto vale tu silencio
		Presión	Skype	Dificultades económicas

Fuente: Elaboración propia

DATE	BEHAVIOUR	APPLICATION INSTANCE	IS/EXPRESSING	MARK
2019-02-14 18:58	PRESSURE	Skype	vacaciones muy costosas	✓
2019-02-14 18:56	RATIONALIZATION	Microsoft PowerPoint - Presentacion estado del proyecto SAP.pptx	ellos tambien roban	✓
2019-02-14 18:52	RATIONALIZATION	Notepad - Carta salario.docx	deseo un sueldo alto	✓
2019-02-14 18:47	PRESSURE	WhatsApp Web	usted no sabe nada	✓
2019-02-14 17:45	PRESSURE	Google Search - Como borrar archivos definitivamente	mi situacion es critica	✓
2019-02-14 17:42	RATIONALIZATION	Microsoft PowerPoint - Presentación junta directiva.pptx	merezco mucho mas	✓
2019-02-14 15:41	PRESSURE	Google Search - Como ganar mas dinero facil y rapido	lo necesito como sea	✓
2019-02-14 15:36	PRESSURE	SAP GUI - Transaccion extranjera	manejas la situacion con cuida...	✓
2019-02-14 15:22	PRESSURE	Skype	cuanto vale su silencio	✓
2019-02-14 14:44	PRESSURE	Skype	dificultades economicas	✓

Figura 4.26 Simulación Víctor Borja

Fuente: (CELCO Cía. Ltda., 2019)

Elaborado por el autor

5 CONCLUSIONES

- El fraude cada vez muta a nuevas formas para lograr su cometido con el apoyo de la tecnología su auge ha tomado fuerza en el área financiera y comercial de las empresas es por eso que las leyes de cada país se intensifican con la finalidad de juzgar y condenar cualquier acto ilícito.
- Como parte de la metodología PMBOK se levantaron los riesgos que pueden afectar al presente proyecto incluyendo a los riesgos.
- La implementación de la herramienta The Fraud Explorer se realizó con éxito y se encuentra operativa lista para cumplir su objetivo que es prevenir y detectar el fraude.
- Las pruebas y simulaciones se realizaron sin ningún problema, la solución es capaz de detectar las palabras asociadas al fraude como demuestran las pruebas realizadas.

6 RECOMENDACIONES

- Se recomienda capacitar al personal que esté a cargo de la administración de la solución con el objetivo que su parametrización este cada vez más acorde al giro del negocio.
- Se aconseja utilizar la metodología PMBOK para el desarrollo de cualquier proyecto se adapta a la necesidad de cualquier proyecto desde estudiantiles hasta macro proyectos industriales.
- Es recomendable realizar una actualización o alcance a la política de la seguridad de la información para que la solución sea parte de ella y realizar una reunión entre las personas interesadas para determinar quiénes serán los responsables de reportar cualquier novedad que reporte la solución.
- Se recomienda la aplicación de la herramienta en otros ámbitos siempre y cuando el objetivo del despliegue de la solución sea para la prevención o detección de fraude u otro delito asociado al mismo, el uso de The Fraud Explorer para otros ámbitos puede derivar en problemas legales entre el usuario y la empresa.
- Es recomendable motivar a los estudiantes a seguir profundizando sobre este tema porque en la actualidad hay poca información sobre como tener una solución como la propuesta y que sea software libre.
- En el futuro se debe analizar el incremento de espacio en disco y memoria RAM en el servidor de The Fraud Explorer.
- Analizar de manera semanal o quincenal los resultados de obtenidos por la herramienta The Fraud Explorer a fin de reportar a través de un informe a la Gerencia General sobre los hallazgos y novedades encontradas.

7 REFERENCIAS BIBLIOGRÁFICAS

- ACFE. (2014). *¿Qué es el fraude?* Retrieved from <https://www.acfe-spain.com/recursos-contrafraude/que-es-el-fraude>
- Alanís, F. (2017). *La Ética Profesional del Ingeniero Civil*. México.
- Appvizer. (2018). *IncMan NG: Software de Cumplimiento de la ley*. Retrieved from <https://www.appvizer.es/justicia/cumplimiento-ley/incman-ng>
- Asamblea Nacional. (2014, Febrero 3). Retrieved from En sesión del 28 de enero del 2014, el Pleno de la Asamblea Nacional conoció
- Auditool. (2016, Junio 2016). *Triángulo del Fraude*. Retrieved from <https://www.auditool.org/blog/fraude/4296-el-triangulo-del-fraude-en-la-cotidianidad>
- Auditool. (2017, Julio 14). *El Diamante del Fraude*. Retrieved from <https://www.auditool.org/blog/fraude/5429-el-diamante-del-fraude>
- Avila, H. (2004). *INTRODUCCION A LA METODOLOGIA DE LA INVESTIGACION*. Mexico.
- CELCO Cía. Ltda. (2015). *Reglamento Interno de Trabajo*. Quito.
- CELCO Cía. Ltda. (2018). *Catálogo de productos*. Retrieved from <http://celco.com.ec/>
- CELCO Cía. Ltda. (2019). *The Fraud Explorer*. Retrieved from <http://thefraudexplorer.celco.com.ec/>
- Chavez, D. (2008, Mayo 21). *CONCEPTOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS EN LA INVESTIGACIÓN*. Retrieved from https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_56.pdf
- Cobo, A., Gómez, P., Pérez, D., & Rocha, R. (2005). *PHP y MySQL*. Retrieved from *Tecnologías para el desarrollo de aplicaciones web*: <http://www.editdiazdesantos.com/wwwdat/pdf/9788479787066.pdf>
- Control Interno y Fraudes. (2006). In R. Estupiñan, *Control Interno y Fraudes con base en los ciclos transaccionales Análisis de informe COSO I y II* (pp. 267-268). Bogota: Ecoe Ediciones.
- Costas, J. (2014). *Seguridad Informática*. Madrid: RA-MA. Retrieved from <http://ebookcentral.proquest.com/lib/uisraelsp/detail.action?docID=3228430>

- Costas, J., & Puche, J. (2010, Diciembre). *Entender el ciclo PDCA de mejora continua*. Retrieved from https://www.aec.es/c/document_library/get_file%3Fp_1_id%3D64199%26folderId%3D195586%26name%3DDLFE-7137.pdf
- Cressey, D. (2017). *THE FRAUD EXPLORER*. Retrieved from www.thefraudexplorer.com/FRAUDE%20EXPLORER/Operaci3n%20%20nfs%20securiy_the-fraud-explorer%20Wiki%20%20GitHub.html
- Del Campo, A. M. (2018, Noviembre 7). *Agile Y Scrum*. Retrieved from Project manager: el puesto de trabajo del que todo el mundo habla: <https://www.iebschool.com/blog/project-manager-agile-scrum/>
- Eguíluz, J. (2008, Diciembre 17). *Introducción a CSS*. Retrieved from https://www.jesusda.com/docs/ebooks/introduccion_css.pdf
- El Binario. (2015, Febrero 19). *Introducción a MariaDB*. Retrieved from https://elbinario.net/wp-content/uploads/2015/02/Introducci%C3%B3n_a_MariaDB1.pdf
- Ernst & Young. (2011). *Seguridad de la información en un mundo sin fronteras*. Mancera.
- Escrivá, G., Romero, R., Ramada, D., & Pérez, R. (2012). *Seguridad Informática*. Madrid.
- Estupiñan, R. (2006). *Control Interno y Fraudes*. Bogota: Ecoe.
- Frett, N. (2014, Septiembre 24). *Tipos de Fraudes*. Retrieved from <https://www.auditool.org/blog/fraude/2981-14-tipos-de-fraudes>
- García, V. (2017). *AUDITORIA FORENSE*. Retrieved from <http://incadesc.com.mx/boletines/Auditoria%20Forense.pdf>
- Gascón, O. (2016). *Ordenando los 49 Procesos de la Guía PMBOK 6*. Retrieved from <https://todopmp.com/49-procesos-pmbok6-ordenados/>
- Gascón, O. (2018). *Guia de certificación PMP*. Retrieved from <https://todopmp.com/>
- Gutierrez, M. (2015, Diciembre 12). *EL AUDITOR INTERNO Y SU RESPONSABILIDAD HACIA EL FRAUDE*. Retrieved from <https://360bestpracticesmethodology.wordpress.com/2015/12/12/el-auditor-interno-y-su-responsabilidad-hacia-el-fraude/>

- Hernandez, E. (2015). *Introducción a Microsoft .NET*. Retrieved from <http://www.disca.upv.es/enheror/pdf/ActaNET.PDF>
- IAI. (2017, Enero). *NORMAS INTERNACIONALES PARA EL EJERCICIO PROFESIONAL DE LA AUDITORÍA INTERNA*. Retrieved from <https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Spanish.pdf>
- INTEF. (2010). *Directivas de Instalación de Software*. Retrieved from http://www.ite.educacion.es/formacion/materiales/85/cd/windows/11Directivas/directivas_de_instalacin_de_software.html
- ISOFT. (2009). *Lenguaje HTML*. Retrieved from <http://www.vc.ehu.es/jiwotvim/ISOFT2010-2011/Teoria/BloqueIV/HTML.pdf>
- LEXIS. (2013). *ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA*. Quito.
- Mayorga, O. (2016). *PREVENCIÓN Y DETECCIÓN DEL FRAUDE EN EL PROCESO DE SUMINISTRO*. Retrieved from <https://repository.javeriana.edu.co/bitstream/handle/10554/21019/MayorgaOjedaOscarFernando2016.pdf?sequence=1>
- Mellado, J. (2015). *Diseños Experimentales*. Retrieved from <http://www.uaaan.mx/~jmelbos/disexp/deapu1a.pdf>
- Ministerio de Justicia. (2012). *Código del Trabajo*. Quito.
- Ministerio de Justicia. (2017). *Código Orgánico Integral Penal*. Quito. Retrieved from https://www.justicia.gob.ec/coip_ed._sdn-mjdhc.pdf
- Mite, I., & Silva, J. (2017). *Estrategias para prevención de riesgos y fraudes en inventarios mediante técnicas de auditoría forense*. Retrieved from <http://repositorio.ug.edu.ec/bitstream/redug/17355/1/Tesis%20Estrategia%20Preencion%20de%20Fraude%20Mite%20-%20Silva.pdf>
- Navarrete, T. (2006, Julio). *El lenguaje JavaScript*. Retrieved from <https://www.dtic.upf.edu/~tnavarrete/fcsig/javascript.pdf>
- NetIQ. (2016). *Amenazas internas: Otros objetivos que ponen en peligro a su empresa*. Retrieved from <https://www.microfocus.com/es-es/media/flash-point->

paper/insider_threats_moving_targets_that_put_your_organization_at_risk_fpp_es.pdf

NF Cybersecurity and Antifraud Firm. (2018). *The Fraud Explorer - Guía de usuario administrador y operador*. Medellín.

NF Cybersecurity and Antifraud Firm S.A.S. (2019, Enero). *Guía de usuario administrador y operador*. Retrieved from https://www.thefraudexplorer.com/files/The_Fraud_Explorer_Userguide.pdf

NFC Security. (2018). *Fuentes The Fraud Explorer*. Retrieved from <https://github.com/nfsecurity/the-fraud-explorer/tree/master/Behavioral%20Harvester>

Palacios, J. (2015). *Análisis de Vulnerabilidades de una Red Corporativa mediante Herramientas de Descubrimiento Activas*. Retrieved from <http://bibing.us.es/proyectos/abreproy/90522/fichero/Memoria+del+Trabajo+Fin+de+Grado.pdf>

Project Management Institute Inc. (2017). *Guía de los FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS*. Pennsylvania.

Rich, E., & Knight, K. (1991). *What Is Artificial Intelligence*. McGraw-Hill.

Ríos, J. (2018). *El triángulo del fraude en la cotidianidad*. Retrieved from <https://www.auditool.org/blog/fraude/4296-el-triangulo-del-fraude-en-la-cotidianidad>

RKward. (2012, Agosto 25). *Documentación del usuario*. Retrieved from https://rkward.kde.org/User_Documentation#General

Rodríguez, M. (2017). *Scrum desde cero*. Madrid: Mc. Graw-Hill.

sadasd. (sdas). *asdas*. sdas: asdsad.

Soberanis, M. d., & Herrera, F. (2018). *XXX CONFERENCIA INTERAMERICANA DE CONTABILIDAD*. Retrieved from <http://www.cpcecba.org.ar/media/img/paginas/La%20Auditor%EDa%20Interna%20En%20La%20Detecci%F3n%20Y%20Prevenci%F3n%20De%20Fraudes.pdf>

Transparency International. (2018). *CORRUPTION PERCEPTIONS INDEX 2018*.

Retrieved from <https://www.transparency.org/cpi2018>

Vasconcelos, S. J. (2014). *Informática 1*. Patria.

Veriato Inc. (2018). *Software de detección de amenazas internas*. Retrieved from

<https://www.veriato.com/products/veriato-recon-insider-threat-detection-software>

8 ANEXOS

Anexo 1. Código Orgánico Integral Penal

Anexo 2. Reglamento Interno de Trabajo CELCO Cía. Ltda.

Anexo 3. Entrevistas

Anexo 4. Acta de Constitución del proyecto

Anexo 5. Registro de Interesados

Anexo 6. Cronograma de gestión e implementación

Anexo 7. Formato de registro incidentes

Anexo 8. Formato de registro incidentes

Anexo 9. Acta de cierre del proyecto

Anexo 10. Pruebas de simulación

Anexo 1. Código Orgánico Integral Penal

Código Orgánico Integral Penal			
Artículo	Delito	Descripción	Observaciones
178	Violación a la intimidad	La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.	No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.
179	Revelación de secreto	La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.	
180	Difusión de información de circulación restringida	La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años.	Es información de circulación restringida: 1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley. 2. La información producida por la Fiscalía en el marco de una investigación previa. 3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.

181	Violación de propiedad privada	<p>La persona que, con engaños o de manera clandestina, ingrese o se mantenga en morada, casa, negocio, dependencia o recinto habitado por otra, en contra de la voluntad expresa o presunta de quien tenga derecho a excluirla, será sancionada con pena privativa de libertad de seis meses a un año.</p> <p>Si el hecho se ejecuta con violencia o intimidación, será sancionada con pena privativa de libertad de uno a tres años.</p> <p>La persona que, en ejercicio de un servicio público, sin la debida autorización o fuera de los casos contemplados legalmente; o que con una orden falsa de la autoridad pública; o que con el traje o bajo el nombre de uno de sus agentes, viole un domicilio o lugar de trabajo, será sancionada con pena privativa de libertad de tres a cinco años.</p>	En la violación de domicilio se presume que no hay consentimiento del dueño o de la dueña o su encargado cuando no están presentes en el acto que constituya la infracción.
186	Estafa	La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.	
187	Abuso de confianza	La persona que disponga, para sí o una tercera, de dinero, bienes o activos patrimoniales entregados con la condición de restituirlos o usarlos de un modo determinado, será sancionada con pena privativa de libertad de uno a tres años.	La misma pena se impone a la persona que, abusando de la firma de otra, en documento en blanco, extienda con ella algún documento en perjuicio de la firmante o de una tercera.

190	Apropiación fraudulenta por medios electrónicos	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.	La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.
192	Intercambio, comercialización o compra de información de equipos terminales móviles	La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.	

Anexo 2. Reglamento Interno de Trabajo CELCO Cía. Ltda.

Reglamento Interno de Trabajo CELCO Cía. Ltda.			
Art.	Items	Descripcion	Numerales/Literales
25	DERECHOS DEL EMPLEADOR	A más de las facultades establecidas en el código del Trabajo y demás normas pertinentes, la Empresa “CELCO CIA. LTDA.”, tendrá, respecto a los trabajadores que prestan servicios en las oficinas, instalaciones y sucursales a su cargo, los siguientes derechos:	<p>4. La Empresa ante los daños, pérdidas, delitos y cuasidelitos que se presenten debido al mal uso de los bienes o incorrecta aplicación de procedimientos, establecerá las responsabilidades correspondientes para los fines de ley, y será considerada dicha falta como grave.</p> <p>7. La Empresa tiene el derecho de instalar cámaras de seguridad que faciliten la vigilancia de los bienes de la misma, estas se instalaran en lugares estratégicos de las instalaciones y no afectara al normal desempeño de las labores de los trabajadores.</p> <p>8. La Empresa podrá utilizar el material procedente de las cámaras de seguridad para usarlas como pruebas de algún tipo de falta cometida a la propiedad o al desempeño de los trabajadores, sin que esto signifique la invasión a la privacidad de los trabajadores que para tal efecto observen faltas a la moral o intimidad de sus funciones.</p>
26	OBLIGACIONES DE LOS TRABAJADORES	Son obligaciones de los trabajadores las consignadas en el Código del Trabajo, de éstas particularidades las señaladas en el artículo 45, como las que establecen en este Reglamento Interno, siendo entre otras las siguientes:	<p>1. Acatar las leyes, reglamentos, políticas, normas, técnicas, manuales, instructivos y demás disposiciones vigentes relacionados con la empresa.</p> <p>4. Abstenerse de toda actividad adicional, lucrativa o no, que pudiere perjudicar o interferir directa o indirectamente, el horario de sus labores.</p> <p>7. Guardar reserva de datos e información confidencial sobre la empresa “CELCO CIA. LTDA.”, cuya elaboración haya sido realizada directa o indirectamente o de aquellos que tenga conocimiento en razón de su trabajo; tanto en el desempeño de sus funciones como en el cese del mismo.</p> <p>11. Fotocopiar, archivar o guardar anotaciones en dispositivos de: Información contable, cartera de clientes, o documentos que el trabajador podría preparar o acceder durante su trabajo, por lo que son de exclusiva propiedad de la Empresa.</p> <p>18. Observar las leyes, reglamentos vigentes de ética profesional, cuando se tratare de un profesional.</p>

			19. Observar lealtad, consideración y respeto para con sus superiores, compañeros y subalternos.
			20. Subordinar el interés personal o particular en beneficio colectivo.
			22. Mantener integridad y decencia en el desempeño de su puesto de tal manera que no ofenda el orden y la moral.
			30. Prestar toda la colaboración posible en caso de siniestro o riesgo inmediato, que afecte o amenace a las personas o bienes de la empresa.
			50. Utilizar los métodos o sistemas de control de tiempo establecidos por la empresa.
27	DE LAS PROHIBICIONES	Prohíbese a los trabajadores de la compañía "CELCO CIA. LTDA.":	2. Desacatar o desobedecer las órdenes, normas e instrucciones dadas por los representantes de la Empresa, sus empleadores, o sus jefes inmediatos durante las horas de trabajo, siempre que las mismas tengan que ver con el objeto normal de sus labores. El trabajador que sin justificación alguna no acatare las órdenes de trabajo emanadas de los superiores, será sancionado con una multa de hasta el 10% de su remuneración mensual. Si el desacato fuere grave, será causal suficiente para solicitar el visto bueno, ante el Inspector del Trabajo competente.
			4. Mantener con los proveedores o compañeros de trabajo, cualquier otra relación que no sea de carácter estrictamente comercial o laboral, se aplica para ello la política de nepotismo para sus colaboradores y proveedores de la Compañía "CELCO CIA. LTDA.".
			5. Ejercer actividades ajenas a las funciones de su puesto de trabajo, durante su horario de labor.
			10. Exigir propinas o recibir coimas u otras ventajas por los servicios prestados.
			11. Solicitar regalos o contribuciones para sí o para sus superiores, o recibirlos de sus subalternos.
			12. Hacer declaraciones a la prensa sobre actividades de la empresa sin autorización expresa.
			13. Desprestigiar o desacreditar a la empresa, funcionarios, empleados o compañeros en general.
			14. Obstaculizar el buen funcionamiento de la empresa.
			15. Divulgar datos confidenciales de la empresa.

		19. Dedicarse a juegos de azar en los sitios de trabajo, incluyendo juegos de vídeo o computación.
		20. Propagar rumores falsos que afecten al buen nombre de la Empresa, de sus funcionarios o de sus trabajadores o que produzcan inquietud entre estos.
		23. Alterar, borrar o rectificar las tarjetas de asistencia, pago de salarios, horas extras, trabajos suplementarios y extraordinarios, marcar la tarjeta de otro trabajador o cualquier otro documento elaborado por la empresa.
		25. Realizar actos que atenten a la moral y buenas costumbres de la empresa, sus compañeros y sus propietarios.
		26. Cometer actos que signifiquen abuso de confianza o fraude.
		27. Ocultar información para evitar que se recaude ingresos para la empresa
		29. Colocar o difundir escritos injuriosos o agredir a sus superiores o a sus compañeros de trabajo de palabra u obra.
		31. Introducir literatura pornográfica, política, subversiva, antipatriótica o lesiva a los intereses de la empresa, reservándose la empresa, el derecho para retirar dicha literatura.
		38. Anotar datos falsos en informes, reportes, etc.
		46. Utilizar la dirección de correos electrónicos, los cuales han sido otorgados como herramienta de trabajo, con el único y exclusivo propósito de facilitar la comunicación de los trabajadores para asuntos relativos al cumplimiento de las tareas o funciones para las cuales han sido contratados.
		47. Hacer competencia a la empresa, comprando, vendiendo, reparando, comercializando, etc., cualquiera de los productos, servicios, equipos, maquinarias, etc., que sean propios de la actividad comercial de la empresa.
		51. Instalar software que no tengan relación con actividades de la empresa, salvo la autorización del administrador de sistemas, quien será en conjunto con el Gerente General, las personas indicadas para autorizar dicha instalación.

			52. Navegar a través de la red en páginas o vínculos que no pertenezcan al giro de negocio de la Empresa, además se prohíbe la descarga de cualquier paquete o utilitario que no sea de correspondencia con la Empresa, El administrador de Sistemas y el Representante Legal son las personas idóneas para autorizar dichas tareas.
33	DISPOSICIONES GENERALES	El incumplimiento al presente Reglamento Interno por parte de los trabajadores será sancionado según la gravedad, con amonestaciones escritas, multas o terminación del contrato de trabajo, de acuerdo a lo señalado en los artículos que siguen.	
			c) Incumplir todas las obligaciones señaladas en el artículo 26 del presente Reglamento.
			d) Violar o no respetar todas las prohibiciones señaladas en el artículo 27 del presente Reglamento.
36	DE LAS FALTAS GRAVES	Se consideran FALTAS GRAVES:	e) Crear rumores, insultos o falta de respeto para sus compañeros o superiores.

Anexo 3. Entrevistas

ENTREVISTA SR. SANTIAGO ARROYO ACCIONISTA DE CELCO CÍA. LTDA.

1) ¿Qué piensa sobre el fraude en general?

Pienso que es algo negativo ya que se hace daño a una persona para beneficio de otra, en general la persona que comete un acto de fraude pierde totalmente credibilidad.

2) ¿Qué es lo primero que se le viene a la cabeza cuando escucha la palabra fraude?

Lo primero que me imagino es a una persona o empresa engañando a otras o robando información para perjudicarlo.

3) ¿Conoce los tipos de fraude que existen?

Conozco el fraude electrónico, fraude bancario y fraude electoral, no estoy seguro cuantos más existan.

4) ¿Cuál es el procedimiento actual cuando hay sospecha de fraude?

Si existe únicamente una sospecha el primer paso es investigar si existe o no fraude y luego si existe fraude dar el siguiente paso que puede ser incluso legal.

5) ¿Cuál es el procedimiento actual cuando se comprueba el fraude?

Dentro de la empresa si se ha comprobado que existe fraude por parte de una persona en primer lugar conversar con esa persona y hacerle saber que conocemos de su acto indebido y se lo retira de la organización, dependiendo de la magnitud se puede seguir un juicio.

6) ¿Qué tipo de medidas pensaría Ud. para prevenir el fraude?

Mejorar los artículos de nuestro manual interno y socializar con el personal en este tema, por otra parte, si se desea prevenir el fraude electrónico colocar restricciones en los computadores.

7) ¿Cree usted que el despliegue de una herramienta informática instalada en la red de CELCO puede aportar para la detección y prevención de fraude?

Creo que si es una opción viable para resguardar la información que la empresa tiene.

8) ¿Estaría dispuesto a invertir en este programa y hasta cuánto?

Si es una herramienta que garantiza la seguridad informática creo que si sería posible, con respecto al costo creo que no debe ser muy costoso ya que la empresa

es mediana, en tema de valores la Gerencia General se encarga de evaluar si el costo beneficio es viable.

9) ¿Qué beneficios cree usted que podría otorgarle a la empresa si se implementaría este sistema?

Resguardar la información y tranquilidad porque se supone la información va estar a buen recaudo sabiendo que si hay intentos de un acto fraudulento nos enteraríamos y no necesariamente se perdería o copiaría información.

10) ¿A mediano plazo cree usted necesaria una auditoría sobre el sistema implementado?

Pienso que una auditoría siempre es necesaria para saber en qué estamos fallando y poder corregir a tiempo, incluso podemos saber si la herramienta falló.

ENTREVISTA SRA. DIANA FERNÁNDEZ GERENTE GENERAL

Las siguientes respuestas fueron resumidas y transcritas, la recolección de la información se grabó durante la entrevista con autorización de la entrevistada.

1) ¿Qué piensa sobre el fraude en general?

Ratifica que es un ataque desleal hacia una empresa o persona y lo asocia a un robo de dinero, producto, información, etc.

2) ¿Qué es lo primero que se le viene a la cabeza cuando escucha la palabra fraude interno?

Piensa que lo primero que se debe realizar es la separación de este mal elemento puesto que puede afectar a su compañía y también a sus compañeros.

3) ¿Conoce los tipos de fraude que existen?

Menciona que el fraude electoral es el que predomina sobre los demás a nivel país, adicional se menciona el fraude financiero, laboral y el soborno en instituciones públicas y privadas.

4) ¿Cuál es el procedimiento actual cuando hay sospecha de fraude?

Reconoce que primero se investiga en su entorno con sus compañeros y se revisa las herramientas corporativas como el correo electrónico.

5) ¿Cuál es el procedimiento actual cuando se comprueba el fraude?

Señala que se toma la decisión de separar a la(s) persona(s) de la compañía y se pone a consideración del departamento legal para que evalúe el caso y si es necesarios tomar acciones legales.

6) ¿Qué tipo de medidas pensaría usted para prevenir el fraude?

Considera que es crítico hablar sobre un proceso de prevención y nos cuenta que los valores personas dependen netamente de cómo fue su vida desde la infancia hasta su edad adulta, adicional menciona que el entorno social, económico y personal influyen a la hora de verse tentados por cometer fraude.

7) ¿Cree usted que el despliegue de una herramienta informática instalada en la red de CELCO puede aportar para la detección y prevención de fraude?

Considera que si puede aportar puesto que dentro de la organización se tiene varias herramientas corporativas como: chats internos, correo electrónico, etc.

8) ¿Estaría dispuesto a invertir en este programa y hasta cuánto?

Nos cuenta que si estaría dispuesta en invertir, pero no nos menciona hasta cuanto invertiría por ser una herramienta fuera de lo común pero si logra ver resultados piensa que se evaluaría una inversión.

9) ¿Qué beneficios cree usted que podría otorgarle a la empresa si se implementaría este sistema?

Manifiesta que los beneficiarios seríamos todos quienes conformamos la organización, al prevenir el fraude se ahorrarían recursos económicos y humanos.

10) ¿A mediano plazo cree usted necesaria una auditoría sobre el sistema implementado?

Considera que todo sistema debe ser auditado a fin de detectar falencias o aciertos del mismo.

	Acta de Constitución del Proyecto	Proyecto:
Fecha: 08/11/2018 Versión: V1.0	Elaborado por: Ronald Coloma	

A. INFORMACION GENERAL

Nombre del Proyecto: IMPLEMENTACIÓN “THE FRAUD EXPLORER FTA” EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE

Patrocinador: Tlga. Diana Fernández, Gerente General

Fecha de Presentación: 08 de noviembre del 2018

HISTORIAL DE VERSIONES

VERSION	PRESENTADO POR	FECHA
1.0	Ronald Coloma	08.11.2018

Autorizado por Propietario del Proyecto: Tlga. Diana Fernández

B. ANTECEDENTES

CELCO Cía. Ltda. se dedicada en proveer soluciones de infraestructura tecnológica de alta confiabilidad y amigables con el medio ambiente
Actualmente la empresa CELCO cuenta con un departamento de sistemas conformado por tres personas, distribuidos de la siguiente manera 1 en la oficina matriz Quito y 2 en Guayaquil.
El fraude ha perjudicado tanto económica y reputacional a la compañía CELCO Cía. Ltda.

C. JUSTIFICACION DEL PROYECTO

Al prevenir fraude interno la organización se protege de personal con malas intenciones lo que beneficiará a la organización porque no se verá afectada económicamente al separar a sus malos elementos mientras que se evita despedir a personal sin motivos o solo por sospechas injustificadas que lo único que puede desencadenar son demandas laborales perjudicando la imagen de la organización.

	Acta de Constitución del Proyecto	Proyecto:
Fecha: 08/11/2018 Versión: V1.0	Elaborado por: Ronald Coloma	

D. REQUISITOS QUE SATISFACEN LAS NECESIDADES, DESEOS Y EXPECTATIVAS DEL CLIENTE, PATROCINADOR Y DEMAS INTERESADOS

D1. Funcionales

- The Fraud Explorer FTA debe estar operativo las 24/7 y los 365 días del año.
- The Fraud Explorer FTA debe monitorear a cada uno de los usuarios que estén dentro del directorio activo.
- The Fraud Explorer FTA debe facilitar la identificación de posibles actores de fraude, a través de reportes.

D2. Técnicos

- Las librerías de palabras a ser monitoreadas deben estar relacionadas con el giro del negocio de la compañía CELCO Cía. Ltda.
- La funcionalidad de reportes debe agrupar a los usuarios por puntaje según el triángulo de fraude de Donald Cressey.
- Los reportes serán enviados a la Gerencia General acompañado de un informe.

E. ALINEAMIENTO DEL PROYECTO A LOS OBJETIVOS ESTRATEGICOS

E1. Objetivos estratégicos a los que contribuirá el Proyecto

- Objetivo Gerencial: Apoyar en la toma de decisiones a la Gerencia en el caso de detectar un fraude interno.
- Objetivo de Administrativo: Generar seguridad al momento de compartir información.

E2. Objetivos del Proyecto

- El despliegue y funcionamiento de la herramienta The Fraud Explorer FTA debe estar lista para el 15 de febrero del 2019.

	Acta de Constitución del Proyecto	Proyecto:
Fecha: 08/11/2018 Versión: V1.0	Elaborado por: Ronald Coloma	

- La implementación y despliegue de la herramienta no debe tener costo.
- El servidor de datos debe estar siempre disponible.

F. GERENTE DEL PROYECTO Y SU NIVEL DE AUTORIDAD

Nombre del Gerente del Proyecto: Ronald Fernando Coloma Andagoya
<p>Responsabilidades principales</p> <ul style="list-style-type: none"> • Elaborar el Plan del Proyecto y asegurar que se cumpla lo establecido. • Llevar a cabo labores de seguimiento y control: Reportar periódicamente la situación del proyecto, actualizar periódicamente el Plan del Proyecto. • Tomar decisiones sobre aspectos que tengan impacto en el alcance, costo o plazo comprometidos. • Asegurar la integridad y calidad de los entregables generados en el proyecto.
<p>Atribuciones principales</p> <ul style="list-style-type: none"> • Tendrá la suficiente autoridad y atribución como para resolver los conflictos que puedan poner en riesgo y los objetivos y metas del proyecto.

G. RESTRICCIONES DE LA ORGANIZACIÓN

<ul style="list-style-type: none"> • El costo de mantenimiento de la herramienta no deberá generar costos directos para la compañía. • Debe garantizarse la integridad y confidencialidad de la información de la empresa. • No se hará ninguna inversión en equipos ni infraestructura tecnológica para el desarrollo del proyecto ni durante el despliegue de la herramienta. • No se hará ninguna inversión en software adicional. • La herramienta debe ser probada por la Gerencia General.

	Acta de Constitución del Proyecto	Proyecto:
Fecha: 08/11/2018 Versión: V1.0	Elaborado por: Ronald Coloma	

H. SUPUESTOS (ASUNCIONES) DE LA ORGANIZACIÓN

<ul style="list-style-type: none"> • La empresa tendrá documentado su requerimiento • La empresa tendrá todos los contenidos (textos, imágenes, videos y audios) en el momento que sea requerido de acuerdo al Plan del proyecto. • Las personas responsables de aprobar los entregables se sujetarán a los plazos establecidos en el Plan del Proyecto.

I. PRESUPUESTO

<p style="text-align: center;">I1.- Costos estimados del Proyecto</p> <ul style="list-style-type: none"> • Materia Prima: 0,00 dólares • Mano de obra: 0,00 dólares • Costos indirectos: 0,00 dólares
<p style="text-align: center;">I2.- Beneficios esperados</p> <ul style="list-style-type: none"> • Identificar a los posibles autores de fraude interno, difamación, robo, complot, etc. • Reducir el número de casos de fraude interno. • Prevenir el fraude para proteger a la compañía de un perjuicio económico o reputacional.

J. PROGRAMA DE HITOS

<ul style="list-style-type: none"> • Iniciación: 08/11/2018 • Planificación: 15/11/2018 • Ejecución: 26/12/2018 • Seguimiento y control: 16/01/2019 • Cierre: 15/02/2019

	Acta de Constitución del Proyecto	Proyecto:
Fecha: 08/11/2018 Versión: V1.0	Elaborado por: Ronald Coloma	

K. INTEGRANTES DEL EQUIPO DEL PROYECTO, ROLES.

Nombre	Rol
Ronald Coloma	Investigador, Implementador y Tester
Ronny Plaza	Analista de fraude
Diana Fernández	Aprobación de entregables

L. FIRMA DE AUTORIZACIÓN DEL ACTA DE CONSTITUCIÓN

Nombre	Cargo	Firma	Fecha
Tlga. Diana Fernández	Gerente General		08/11/2018

Anexo 5. Registro de Interesados

Registro de Interesados						
Versión 1.0						
Nombre y Apellido	Empresa	Cargo	Ubicación	Información de contacto	Grado de interés	Etapas de interés
Diana Fernandez	CELCO	Gerente General	Guayaquil	diana.fernandez@celco.com.ec	Alto	Implementación
Edgar Arroyo	CELCO	Presidente	Guayaquil	edgar.arroyo@celco.com.ec	Alto	Implementación
Santiago Arroyo	CELCO	Accionista	Quito	santiago.arroyo@celco.com.ec	Medio	Implementación
Danilo Arroyo	CELCO	Accionista	Quito	danilo.arroyo@celco.com.ec	Medio	Implementación
Xavier Arroyo	CELCO	Jefe de Sistemas	Guayaquil	xavier.arroyo@celco.com.ec	Alto	Ejecución
Ronny Plaza	CELCO	Asistente de Sistemas	Guayaquil	ronny.plaza@celco.com.ec	Alto	Ejecución y control
Ronald Coloma	CELCO	Asistente de Sistemas	Quito	ronald.coloma@celco.com.ec	Alto	Gestión y desarrollo

ACTA DE CIERRE DEL PROYECTO

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
IMPLEMENTACIÓN “THE FRAUD EXPLORER FTA” EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE	I.T.F.E.C
NOMBRE DE EMPRESA	
CELCO Cía. Ltda.	

DECLARACIÓN DE LA ACEPTACIÓN FORMAL	
<p>Por la presente se deja constancia de que el Proyecto I.T.F.E.C ha sido aceptado y aprobado por el beneficiario del proyecto la Tlga. Diana Fernández Gerente General de la empresa CELCO Cía. Ltda., por lo que concluye que el proyecto ha sido culminado exitosamente.</p>	
<p>El proyecto comprendía de la entrega de los siguientes entregables:</p> <ul style="list-style-type: none">• Herramienta The Fraud Explorer implementada y funcionando• Copia del proyecto escrito	
OBSERVACIONES ADICIONALES	
<p>El proyecto ha sido desarrollado dentro de los tiempos planificados, siendo la fecha de término en la planificación 28 de Febrero de 2019.</p>	
ACEPTADO POR	
<i>NOMBRE DE LA EMPRESA</i>	<i>FECHA</i>
CELCO Cía. Ltda.	28 de Febrero de 2019

DISTRIBUIDO Y ACEPTADO	
<i>NOMBRE DEL STAKEHOLDER</i>	<i>FECHA</i>
Diana Fernández	15 de Febrero de 2019
Santiago Arroyo	15 de Febrero de 2019

Entrega conforme

Ronald Coloma

Reciben conforme

Diana Fernández

Anexo 9. Registro de lecciones aprendidas

REGISTRO DE LECCIONES APRENDIDAS										
Nro. Ref.	Código de Proyecto	Nombre del Proyecto	Área / Categoría	Fecha	Amenaza / Oportunidad	Título	Descripción de la Situación	Descripción del Impacto en los objetivos del proyecto	Acciones Correctivas y Preventivas Implementadas	Lección Aprendida / Recomendaciones
RL01	I.T.F.E.C	IMPLEMENTACIÓN “THE FRAUD EXPLORER FTA” EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE	Cierre del proyecto	05/02/2019	Oportunidad	Instalacion y Configuracion de The Fraud Explorer	Para la implementacion de la herramienta The Fraud Explorer es necesario conocer sobre virtualizacion de maquinas y servidores en el sistema operativo Linux, PHP, Elastic y Active Directory	Genera nuevos conocimientos	Como accion preventiva se recomienda desarrollar un documento que incluya la instalacion y configuracion de la herramienta	Implementar un manual de administracion para la configuracion de la herramienta
RL02	I.T.F.E.C	IMPLEMENTACIÓN “THE FRAUD EXPLORER FTA” EN LA EMPRESA CELCO CÍA. LTDA. COMO MECANISMO DE PREVENCIÓN Y DETECCIÓN DE FRAUDE	Cierre del proyecto	05/02/2019	Oportunidad	Administracion de The fraud Explorer	Para la administración de la herramienta The Fraud Explorer es necesario conocer sobre el funcionamiento y como interpretar los resultados obtenidos.	Genera nuevos conocimientos	Como accion preventiva se recomienda desarrollar un documento que incluya los pasos para el ingreso y monitoreo de los usuarios	Implementar un manual de usuario

Anexo 10. Pruebas de simulación

← → ↻ <https://thefraudexplorercelco.com.ec/eventData?endpoint=YW1GemlyND0=> ☆ 📄 🏠 🌐

NF Dashboard Fraud Triangle Events Analytics Endpoints Rules Roles Setup Maintenance Offline 0015 Online 0000 Total 0015 Search ... 🔍 Logout

☰	📅 DATE	BEHAVIOUR	📄 APPLICATION INSTANCE	🔍 IS/EXPRESSING	MARK
👤	2019-02-14 18:58	PRESSURE	Skype	✓ vacaciones muy costosas	✓
👤	2019-02-14 18:56	RATIONALIZATION	Microsoft PowerPoint - Presentacion estado del proyecto SAP.pptx	✓ ellos tambien roban	✓
👤	2019-02-14 18:52	RATIONALIZATION	Notepad - Carta salario.docx	✓ deseo un sueldo alto	✓
👤	2019-02-14 18:47	PRESSURE	WhatsApp Web	✓ usted no sabe nada	✓
👤	2019-02-14 17:45	PRESSURE	Google Search - Como borrar archivos definitivamente	✓ mi situacion es critica	✓
👤	2019-02-14 17:42	RATIONALIZATION	Microsoft PowerPoint - Presentación junta directiva.pptx	✓ merezco mucho mas	✓
👤	2019-02-14 15:41	PRESSURE	Google Search - Como ganar mas dinero facil y rapido	✓ lo necesito como sea	✓
👤	2019-02-14 15:36	PRESSURE	SAP GUI - Transaccion extranjera	✓ manejes la situacion con cuida...	✓
👤	2019-02-14 15:22	PRESSURE	Skype	✓ cuanto vale su silencio	✓
👤	2019-02-14 14:44	PRESSURE	Skype	✓ dificultades economicas	✓

There are 25 regular expressions matched ⏮ 1 to 25 of 25 records ⏭ by 50 events Download as CSV

The Fraud Explorer® Opensource Fraud Triangle Analytics [Bug Report](#) [Documentation](#) [Take tour](#) [Support](#) [Company \[admin - all\]](#) [Version v1.2.2-ai](#)

Fuente: The Fraud Explorer CELCO Cía. Ltda.
Elaborado por el autor

← → ↻ <https://thefraudexplorercelco.com.ec/eventData?endpoint=Ym1sbpXdz0=> ☆ 🏠 🗄️ | T ⋮

NF Dashboard Fraud Triangle Events Analytics Endpoints Rules Roles Setup Maintenance Offline 0005 Online 0010 Total 0015 Search ... 🔍 Logout

	DATE	BEHAVIOUR	APPLICATION INSTANCE	IS/EXPRESSING	MARK
📄	2019-02-14 16:14	PRESSURE	Google Search - Represion en el trabajo	✓ crisis en la empresa	✓
📄	2019-02-14 15:42	PRESSURE	Skype	✓ vigilan el tiempo	✓
📄	2019-02-14 15:25	PRESSURE	Microsoft Word - Listado de proveedores ultimo semestre.docx	✓ cumplir dentro del plazo	✓
📄	2019-02-14 13:24	PRESSURE	Google Search - Como desprestigiar a mi jefe	✓ estoy bajo mucha presion	✓
📄	2019-02-14 12:47	PRESSURE	Microsoft Word - Documento de comunicacion personal.docx	✓ usted nunca supo nada	✓
📄	2019-02-14 11:52	PRESSURE	Yahoo Preguntas - Mi jefe el sapo	✓ maneje la situacion con mucha...	✓
📄	2019-02-14 11:44	PRESSURE	Google Search - Como borrar archivos definitivamente	✓ mi situacion es critica	✓
📄	2019-02-14 11:40	PRESSURE	Microsoft Project - Cronograma ajustado proyecto Azul.mpp	✓ estan espiando	✓
📄	2019-02-14 11:31	PRESSURE	Microsoft Project - Proyecto construccion casa.mpp	✓ dejese querer	✓
📄	2019-02-14 11:27	PRESSURE	Microsoft Excel - Resumen de finanzas personales.xlsx	✓ problemas con la familia	✓

There are 25 regular expressions matched ⏪ 1 to 25 of 25 records ⏩ by 50 events ⌵ Download as CSV

The Fraud Explorer © Opensource Fraud Triangle Analytics [Bug Report](#) [Documentation](#) [Take tour](#) [Support](#) [Company \[admin - all\]](#) [Version v1.2.2-ai](#)

Fuente: The Fraud Explorer CELCO Cía. Ltda.
Elaborado por el autor