UNIVERSIDAD HISPANOAMERICANA

ESCUELA DE INGENIERÍA INFORMÁTICA

TESIS PARA OPTAR POR EL GRADO ACADÉMICO DE LICENCIATURA EN INGENIERIA INFORMÁTICA

MODELO DE PERFIL Y COMPORTAMIENTO TRANSACCIONAL EN LA DETECCIÓN DE FRAUDES EN EL SISTEMA BANCARIO

Sustentante:
Abraham Cerdas Arce

Tutor:
Esteban Quirós Valverde

Febrero, 2019

ÍNDICE DE CONTENIDO

CONTENIDO

Índice de Figuras

Índice de Tablas

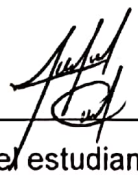
Índice de Anexos

DECLARACIÓN JURADA

Yo Abraham Cerdas Arce, mayor de edad, portador de la cédula de identidad número 1-1340-0687 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática, juro solemnemente que mi trabajo de investigación titulado: Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario.

_____, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 25 días del mes de Febrero del año dos mil 19.



Firma del estudiante

Cédula: 1-1340-0687

22 de febrero del 2019

Señora
Marylin Arias Soto
Directora Ingeniería Informática
Universidad Hispanoamericana

Estimada Señora:

El estudiante Abraham Cerdas Arce, cédula de identidad 1-1340-0687, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "**MODELO DE PERFIL Y COMPORTAMIENTO TRANSACCIONAL EN LA DETECCIÓN DE FRAUDES EN EL SISTEMA BANCARIO"**, el cual ha elaborado para optar por el grado académico de Licenciatura.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación, antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos, conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

N°	ASPECTO A EVALUAR	VALOR	OBTENIDO
a)	ORIGINALIDAD DEL TEMA	10%	9%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
c)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACIÓN	30%	28%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	18%
e)	CALIDAD, DETALLE DEL MARCO TEÓRICO	20%	18%
TOTAL			**93%**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

ESTEBAN ROBERTO QUIROS VALVERDE (FIRMA)

Firmado digitalmente por ESTEBAN ROBERTO QUIROS VALVERDE (FIRMA)
Fecha: 2019.02.22 11:14:30 -06'00'

Ing. Esteban Roberto Quirós Valverde, MAP
Cédula de identidad N° 1-1211-0045
Carné Colegio Profesional 3199

UNIVERSIDAD HISPANOAMERICANA

CARTA DEL LECTOR

Heredia, 4 de Mayo del 2019

A quien corresponda
Director Ingeniería Informática
Universidad Hispanoamericana

Estimado Señor:

El estudiante ABRAHAM CERDAS ARCE, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "**MODELO DE PERFIL Y COMPORTAMIENTO TRANSACCIONAL EN LA DETECCIÓN DE FRAUDES EN EL SISTEMA BANCARIO**", el cual ha elaborado para optar por el grado de Licenciatura.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y el análisis de datos; la consistencia de los datos recopilados y la coherencia de estos y las conclusiones; así mismo la aplicabilidad y originalidad de las recomendaciones en términos de aporte de la investigación.
He verificado que se han hechos las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atentamente,

Ing. Erick López Chavarria, M.R.I.
Cédula 1-0993-0088

Vázquez de Coronado, 15 de mayo 2019

A quien corresponda:

Por medio de la presente hago constar que leí y corregí el Trabajo Final de Graduación, denominado: **"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario"** elaborado por el estudiante **Abraham Cerdas Arce**; para optar al grado de Licenciatura en Ingeniería Informática.

Corregí el trabajo en aspectos tales como: construcción de párrafos, vicios del lenguaje que se trasladan a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico, y desde ese punto de vista considero que, una vez realizados los cambios recomendados, estará listo para ser presentado como Trabajo Final de Graduación.

Suscribe cordialmente,

Bach. Kattia Elena Barrientos Quirós
Céd.: 1-13330834
Carné 160 Asociación Costarricense de Filólogos
Filóloga

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 26 de Julio de 2019

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Abraham Cerdas Arce con número de identificación 1-1340-0687 autor (a) del trabajo de graduación titulado Modelo Perfil y Comport. Trans. presentado y aprobado en el año 2019 como requisito para optar por el título de Licenciatura ; (SI/ NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

1-1340-0687
Firma y Documento de Identidad

DEDICATORIA

El inicio y fin de este proyecto está dedicado primeramente al esfuerzo y a la perseverancia en la culminación de mi carrera profesional, siendo Dios el pilar más importante para cumplir con el objetivo.

A mi familia, principal fuente de inspiración, que con amor me ha acompañado en todo momento, apoyándome en cada una de las etapas educativas, brindándome ideales de superación y de realización de metas.

AGRADECIMIENTOS

Agradezco primeramente a Dios por darme la vida y la salud para poder realizar mis metas.

A mi familia, por estar siempre a mi lado en los momentos más importantes de mi vida. Este logro también es de ustedes.

A mi patrono, que me ha brindado un soporte económico estable durante años laborales y la flexibilidad para finalizar mis estudios.

Amigos, que han sido fuente de inspiración.

Profesores, que se han tomado el tiempo de transmitirme sus conocimientos con un estilo pedagógico de excelencia.

Al señor tutor el Lic. Esteban Quirós por su profesionalismo y orientación en el desarrollo del proyecto

INTRODUCCIÓN

Si nos preguntáramos cómo funciona nuestro cerebro, posiblemente obtendríamos diversas respuestas y criterios al respecto, tanto desde el punto de vista profesional y científico como desde la experiencia personal. En tal caso, es nuestro nivel de razonamiento quien nos ayudará a obtener diferentes puntos de vista para llegar a entender la estructura que utilizamos al momento de analizar todo lo que hacemos.

Esta capacidad de raciocinio nos ha permitido desarrollar una tecnología propia la cual se encuentra, en estos momentos, orientada a descubrir su origen mediante la evaluación de las siguientes preguntas: ¿Cómo funciona el cerebro? ¿Se pueden construir modelos computacionales artificiales que lo emulen? ¿Se pueden desarrollar máquinas inteligentes? Todas estas preguntas han conducido a un desarrollo exponencial de un campo multidisciplinar del conocimiento conocido como Inteligencia Artificial.

Este proyecto tiene como propósito analizar el uso de redes neuronales enfocándose en *Machine Learning* y *Deep Learning* en la detección de fraudes en el sistema bancario, basándose en los principales conceptos de inteligencia artificial, los cuales serán mencionados más adelante (a lo largo del documento); por otro lado, es importante mencionar que el modelo y las reglas de negocio que se desarrollaran en este documento para la solución del proyecto, tendrán como finalidad definir las pautas y procedimientos para la prevención y detección de fraudes, facilitando a los altos mandos la toma de decisiones con el fin de realizar los ajustes pertinentes en su estructura de seguridad.

CAPÍTULO I:

PLANTEAMIENTO DEL TEMA

1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

1.1.1 Antecedentes del Contexto de la Empresa

En la actualidad, las entidades financieras en Costa Rica requieren acciones estratégicas que les permitan mejorar la forma en que brindan sus productos a los clientes, enfocándose en temas de practicidad, accesibilidad y seguridad. Este último enfoque, será el más importante para el desarrollo del proyecto, de tal forma que abarcará mucha información de aspectos teóricos y técnicos que permitirán mejorar la usabilidad de los productos.

A efectos de conocer cómo funciona a nivel de la seguridad de la información una entidad financiera, se utilizará como referencia al Banco Nacional de Costa Rica, sin embargo, para el desarrollo de la investigación serán evaluados el sector financiero en general y sus principales indicadores, considerando tanto instituciones públicas como privadas.

A continuación, la información respectiva del banco:

- **Nombre de la Empresa:**
  Banco Nacional de Costa Rica.

- **Año de fundación**
  09 de octubre de 1914.

- **Misión:**
  "Mejorar la calidad de vida del mayor número de personas, ofreciendo servicios financieros de excelencia, que fomenten la creación sostenible de riqueza" (Banco Nacional de Costa Rica, 2018).

- **Visión:**
  "Ser el mejor Banco del país en servicio al cliente" (Banco Nacional de Costa Rica, 2018).

- **Objetivos:**

  El Banco Nacional de Costa Rica está comprometido con el desarrollo económico, social y ambiental. Adopta las mejores prácticas de Responsabilidad Social en su estrategia Gerencial, su cadena de valor, su entorno inmediato y en concordancia con las iniciativas del país. Asegura, con ello, los recursos que permiten su nivel de competitividad y refuerza el dialogo estructurado con los públicos de interés, para lograr su desarrollo sostenible en el mediano y largo plazo. (Banco Nacional de Costa Rica, 2018)

  El Banco Nacional de Costa Rica, como líder del sector financiero costarricense, reconoce la importancia y el impacto real y potencial de sus acciones sobre el desarrollo sostenible del país. En consecuencia, hace suyo el objetivo nacional de alcanzar la neutralidad de carbono en el año 2021, y se identifica con el compromiso de Costa Rica de conservar al máximo posible sus recursos de agua, suelos y biodiversidad para las futuras generaciones. (Banco Nacional de Costa Rica, 2018)

- **Negocio al que se dedica:**

  El Banco Nacional de Costa Rica se dedica a la captación de fondos los cuales juntamente con el capital propio del banco son canalizados o colocados a sus clientes, mediante la cartera de servicios financieros, teniendo como fin el desarrollo integral económico.

- **Historia de la organización.**

  A comienzos de la primera guerra mundial, nace en Costa Rica en 1914 el primer banco estatal bajo la administración del presidente Alfredo González Flores. En aquella época la situación financiera del país requería de algunos cambios de manera que las familias costarricenses tuvieran accesibilidad a una moneda propia bajo estándares públicos, esto

con el fin de prevenir una posible contracción de las exportaciones, de este modo, la principal motivación por parte del gobierno era estimular la demanda interna.

Al pasar de los años existieron varias administraciones que le dieron un enfoque emisor, comercial e hipotecario, sin embargo, este enfoque vino a cambiar con la descentralización propuesta por uno de los últimos gerentes generales (1997-2009). Él propuso la idea de crear seis bancos regionales y tres subsidiarias, asentando de este modo las bases del esquema que actualmente posee la institución con el actual nombre de Banco Nacional de Costa Rica. Además, gracias a su creación surgieron otras entidades financieras y gubernamentales que han aportado beneficios a los ciudadanos costarricenses.

1.1.2 Justificación del Proyecto

En los últimos años el uso de herramientas tecnológicas en el sistema bancario ha tomado un valor significativo en la operación transaccional de los clientes, en consecuencia, han surgido grupos organizados de personas que han hecho un uso ilícito de dichas herramientas. Por esta razón, los entes financieros están constantemente actualizando sus sistemas e informando a sus clientes sobre este tipo de eventos, sin embargo, la vulnerabilidad que recae sobre ellos fuerza a los bancos a tomar acciones más severas que protejan la integridad de la información de los usuarios y así velar por la confianza que se tiene en el banco para que mantengan activos en sus carteras ya sea de inversiones o de financiamiento.

Por un lado, según datos del Banco de México (Banxico) revelados en el 2015, el robo de identidad va en aumento y el país ya ocupa la posición número ocho a nivel mundial en este delito. Según datos de Condusef en el 2016, se registraron 78,788 posibles casos. La mayoría de los casos se registraron en contra del Grupo Financiero CitiBanamex (Alonso, 2017, párr. 5)

Por otro lado, Condusef informó que, durante el primer trimestre del 2017, se registraron 1.5 millones de reclamaciones por fraude en el sector bancario, es decir, prácticamente 18,000 por día, lo cual representa un aumento de 10% respecto al mismo periodo del 2016" (Alonso, 2017, párr. 9)

En referencia a la información anterior, Costa Rica tampoco escapa de este tipo de datos, el diario La Nación en el 2017 publicó en varios artículos las diferentes formas en que los delincuentes comenten fraudes, estafas y suplantaciones para perjuicio de varios usuarios del sistema bancario nacional.

Por tales razones, el análisis y desarrollo de las redes neuronales basadas en el *modelo de perfil y comportamiento transaccional* se proponen como una solución más en este proyecto. El objetivo es: que se permita disminuir considerablemente que los grupos organizados saquen ventaja de falta de la información y la negligencia de los usuarios; además, que se pueda proveer al sistema bancario lineamientos puntuales de inteligencia del negocio relacionados a las estructuras de seguridad informática, fortaleciendo, mediante recopilación de experiencias, los sistemas que actualmente se están utilizando.

1.2 DEFINICIÓN DEL PROBLEMA

En los últimos años el sistema bancario nacional ha implementado una serie de servicios mediante canales electrónicos, siendo los más sobresalientes sitios web y *apps* para dispositivos móviles, los cuales están orientados a facilitar la operativa y la trazabilidad que demandan los clientes, sin embargo, las posibilidades de verse afectados por fraudes aumentan considerablemente debido a la alta recurrencia de ataques al sistema tratando de vulnerabilizar los mecanismos de seguridad que traen como consecuencias directas perjuicios económicos.

Las nuevas tendencias tecnologías, las diferentes propuestas presentadas por las industrias que brindan servicios informáticos junto con el cambio de mentalidad de los clientes en un mundo de gran crecimiento digital, obligan a los sectores financieros a renovar sus estructuras o la forma en que ofrecen sus servicios, dejando en un segundo plano el método tradicional en donde un altísimo porcentaje de clientes llegaban a sus oficinas. Ahora, Con el fin de ampliar puntualmente la situación que se presenta en la actualidad, a continuación se presenta el siguiente diagrama.

1.2.1 Diagrama de Causa y Efecto.

Figura 1: Diagrama de Causa y Efecto
Fuente: https://www.bncr.fi.cr

La definición del problema parte de la consolidación de un evento delictivo, el cual se denomina materialización del fraude informático, sin embargo, la idea principal de este diagrama de causa y efecto es poder identificar los factores que intervienen, sin afán de explicar una solución de este.

A pesar de que el Banco Nacional de Costa Rica tiene mecanismos de detección, existen causas que dificultan poder eliminar el fraude, razón por la cual se derivan de ello varios efectos que a manera de explicación podrán contemplarse más adelante en el desarrollo del proyecto.

1.3 OBJETIVOS DEL PROYECTO.

1.3.1 Objetivo General

- Desarrollar un modelo de perfil y comportamiento transaccional para la detección de fraudes en la estructura de seguridad informática del Banco Nacional de Costa Rica.

1.3.2 Objetivos Específicos

- Identificar las principales vulnerabilidades presentadas por los usuarios ante un fraude en función de los servicios en línea o presenciales que utiliza.

- Justificar el proceso de detección de fraudes que se emplea en una entidad financiera enfocado en la aplicación de entrevistas en las plataformas de servicios.

- Valorar el perfil de los clientes y su comportamiento transaccional brindando criterios de análisis relacionados a los métodos de clasificación de la entidad financiera como segmentación, actividad económica e información bancaria.

- Establecer una guía de supervisión periódica que muestre indicadores de mejora en todas las áreas expuestas a eventos maliciosos por medio de experiencias.

1.4 ALCANCES Y LIMITACIONES

1.4.1 Alcances del Proyecto.

- Se pretende identificar mediante evaluaciones, las principales causas en las que los usuarios se ven vulnerables, con el fin de tener un diagnostico actual de la situación y poder determinar las acciones inmediatas que se ejecutaran durante el desarrollo del proyecto.

- La investigación abarca únicamente los procedimientos, protocolos o normativas que utiliza el Banco Nacional de Costa Rica para la detección de fraudes en sus estructuras de seguridad informática, con el fin de poder compararlos o bien buscar oportunidades de mejora para que sean más eficientes y completos.

- Los nuevos avances en la inteligencia artificial permiten ser compatibles con tecnologías ya existentes, por ende, se analizan las opciones de fusionar este modelo de red neuronal con la forma en que actualmente el Banco Nacional de Costa Rica registra los eventos.

- El desarrollo del proyecto no contempla la elaboración de un software, sino, definir un modelo de reglas de negocio que le permita a la organización encargada de la seguridad informática tener una forma más precisa de registrar los eventos en bitácoras o bases de datos, los cuales estén relacionados a fraudes, por ende, no entra dentro del PETI (Plan Estratégico de TI).

- Parte del proceso de desarrollo del modelo es considerar, una vez establecido, un cronograma de supervisión de mejora continua, con el fin de fortalecer aquellas áreas que podrían verse afectadas o bien violentadas, esto mediante una comisión o departamento estratégico.

1.4.2 Limitaciones del Proyecto

- Para mantener la integridad y confidencialidad de la información se presentarán datos y casos que ayudarán a explicar la realización del proyecto, sin embargo, no se detallara la identidad de los usuarios involucrados.

- Como entidad pública se tienen que respetar ciertos criterios, políticas y normativas, de manera que no se podrán modificar aun cuando el análisis del proyecto lo permita.

- La información que se analizara no está actualizada, ya que dependen de otros departamentos el registro de los eventos, al momento de la realización de la investigación.

- El soporte brindado por parte del Banco será únicamente con los departamentos de seguridad bancaria y seguridad de la información, aunque se requiera de un asesoramiento externo, las políticas de control interno y auditoria no lo permite

CAPÍTULO II:

MARCO TEÓRICO

2.2 MAPA CONCEPTUAL

2.2.1 Definiciones Generales

2.2.1.2 Modelo de Perfil

Un modelo es: “Esquema teórico, generalmente en forma matemática, de un sistema o de una realidad compleja, como la evolución económica de un país, que se elabora para facilitar su comprensión y el estudio de su comportamiento” y perfil es: “Conjunto de rasgos peculiares que caracterizan a alguien o algo” (rae, 2018). La fusión de estos términos nos permite aplicar a este proyecto un concepto específico e informático que caracterice la situación de un individuo.

2.2.1.3 Comportamiento Transaccional

Para efectos del proyecto, el comportamiento transaccional estará enfocado en la relación operativa y comercial que tendrá un cliente con la entidad financiera, para ampliar el enfoque podemos relacionar el comportamiento transaccional al perfil transaccional de un individuo.

Según la Superfinanciera (Superintendencia Financiera de Colombia), el perfil transaccional permite conocer cuáles son los hábitos de un consumidor financiero, por ejemplo, los canales que usa, los montos y días de retiro, los lugares en que se realizan, y a partir de allí, cada entidad es autónoma en definir un procedimiento con el cual se confirmen las operaciones que no correspondan a los hábitos transaccionales del cliente, y con ello generar la alerta respectiva. (Fierro, 2017)

Asimismo, en sentencia del 27 de octubre del 2016, expediente 11001319900120150020601 del boletín jurídico número 65, la Superintendencia Financiera de Colombia (2016) reafirma:

> El perfil transaccional es el resultado del análisis de experiencias a cuya reiteración en el tiempo el ordenamiento quiso darle efectos propios. Así en línea de principio, el titular de un producto bancario no asume pérdidas por las operaciones que no ha realizado, incluso cuando culposamente ha facilitado a terceros que las realicen, cuando las mismas se separen de sus costumbres transaccionales. Podría decirse, con recurso a la figura, que el perfil transaccional es a las operaciones bancarias lo que la huella dactilar es a cada individuo. (párr. 5)

En Costa Rica, la SUGEF (Superintendencia General de Entidades Financieras) hace referencia al perfil y comportamiento del cliente, indicando una de sus funciones:

> Las Superintendencias pueden realizar las comprobaciones pertinentes para verificar que la metodología de clasificación de riesgo de los clientes es razonable de acuerdo con el volumen y naturaleza de las operaciones que lleva a cabo el sujeto fiscalizado, así como al perfil de cliente que atiende. La Superintendencia correspondiente debe requerir al sujeto fiscalizado que tome las medidas que corresponda para su corrección, aclaración o sustitución en el plazo que ésta establezca. (SUGEF, 2010, p. 10)

Teniendo en cuenta ambos criterios, el comportamiento transaccional de un cliente es un aspecto fundamental para las entidades financieras, el cual debe ser analizado desde diferentes puntos de vista, de manera que se determine la actividad normal acorde a su rango de ingresos y movimientos.

Durante el desarrollo del proyecto, el perfil transaccional o comportamiento transaccional será evaluado con diferentes teorías de inteligencia de negocio sin descuidar, desde un enfoque operativo, las posibles inconsistencias o amenazas que se pueden presentar.

2.2.1.4 Fraude

El fraude es uno de los medios más comunes utilizados por aquellas personas que buscan apropiarse de bienes materiales o bien, de información sensible e importante; para tales efectos el engaño es el *modus operandi*, de tal forma que la víctima nunca se imagina el daño que está por venir.

La Asociación de Examinadores de Fraude Certificados [ACFE] (2018) clasifican los fraudes en tres principales tipos:

1. **Fraude Interno:**

   Este tipo de fraude se produce cuando un empleado, gerente, o ejecutivo comete fraude en contra de su empleador.

2. **Fraude Externo:**

   Este tipo de fraude cubre una amplia gama de esquemas, desde vendedores y clientes deshonestos hasta terceros desconocidos que atenten contra la seguridad y propiedad intelectual.

3. **Fraude Contra Personas:**

   Este tipo de fraude básicamente se resume a un acto contra personas. Robo de identidad, *phishing,* pagos por adelantados, entre otros son ejemplos de este fraude.

Aunque existen varios tipos de fraude, esta investigación se basará en dos en específico: el fraude informático y fraude financiero. Ambos se contemplan en los tres principales tipos de fraude

mencionados por la ACFE, reuniendo varias de las características he impactos, por ende, será relacionado a delitos informáticos ocasionados a personas bajo un ambiente financiero o directamente dirigidos a instituciones bancarias.

2.2.1.5 Fraude Informático

El fraude informático utiliza medios electrónicos para hacerse de datos o del control de datos confidenciales que permiten cometer el acto ilícito y estafar a los usuarios, formato reconocido como *hacking*. Otra manera de cometer un fraude cibernético es por medio de la intercepción de datos por medios electrónicos, donde si bien no hay un engaño dirigido a una determinada persona, sí hay una violación de privacidad y un uso malicioso de la información recolectada. En este sentido, la obtención de contraseñas, cuentas de tarjetas de crédito o datos confidenciales sobre la identidad de una persona, conforman el tipo de información requerida para quien tiene la intención de cometer una estafa.

En Costa Rica el fraude informático es penado con un mínimo de seis meses de prisión según lo indican los siguientes artículos, antes se debe recalcar que de estos el 217 es el más severo, La Asamblea Legislativa de la Repúblia de Costa Rica (2001), determina:

- "Artículo 196 bis. -Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años”

- "Artículo 217 bis. -Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de

cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

- "Artículo 229 bis. -Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años”

2.2.1.6 Fraude Financiero

El fraude financiero se da en un entorno profesional y económico. No se presenta el uso de la violencia, pero sí se ocasionan pérdidas económicas a empresas, compañías, inversores, empleados y clientes.

Es importante destacar que en los últimos años las pérdidas económicas ocasionadas por actos delictivos de esta índole han causados gran impacto en la cartera de clientes de diferentes organizaciones, las principales han sido las entidades bancarias y financieras.

2.2.2 Definiciones Técnicas

2.2.2.1 Inteligencia Artificial

La forma en que el cerebro humano realiza sus funciones y ejecuta acciones para materializar lo que se quiere, es la principal fuente o insumo que utiliza la inteligencia artificial para alimentar una máquina y hacer que esta aprenda, teniendo la autosuficiencia de emitir un resultado bajo su propio criterio.

Salesforce (2018) la define de este modo: “Inteligencia artificial es el concepto para máquinas que “piensan como seres humanos”; en otras palabras, que realizan tareas como: razonar, planificar, aprender y entender el lenguaje” (párr.4)

2.2.2.2 Redes Neuronales

Las Redes Neuronales son un campo muy importante dentro de la Inteligencia Artificial. Estas se inspiran en el comportamiento conocido del cerebro humano (principalmente el referido a las neuronas y sus conexiones), trata de crear modelos artificiales que solucionen problemas difíciles de resolver mediante técnicas algorítmicas convencionales.

Por ejemplo, si se saben los píxeles de una imagen habrá una forma de saber qué número hay escrito; o conociendo la carga de servidores de un Centro de Procesamiento de Datos (CPD), su temperatura y demás, existirá una manera de saber cuánto van a consumir, de esta misma forma lo hacía Google. El problema, claro está, es que no sabemos cómo combinarlos. (Julian, 2014, párr. 4)

Siguiendo con la definición, las redes neuronales son un modelo para encontrar esa combinación de parámetros y aplicarla al mismo tiempo. En el lenguaje propio, encontrar la combinación que mejor se ajusta es "entrenar" la red neuronal. Una red ya entrenada se puede usar luego para hacer predicciones o clasificaciones, es decir, para "aplicar" la combinación. (Julian, 2014, párr. 5)

2.2.2.3 Red de Contra Propagación

Es un algoritmo de aprendizaje supervisado, para el entrenamiento de perceptrones multicapa (redes neuronales artificiales), con el objetivo de que resultados no deseados sean reingresados y analizados con el fin de brindar un resultado positivo.

El algoritmo *backpropagation* busca el valor mínimo de la función de error en el espacio de peso utilizando una técnica llamada regla delta o pendiente de gradiente. Los pesos que minimizan la función de error se consideran una solución al problema de aprendizaje.

2.2.2.4 Inteligencia del Negocio (BI)

Cuando se desea analizar una gran cantidad de datos y que estos se conviertan en información con significado para dar una respuesta ante una situación dada, se deben aplicar ciertas herramientas que facilitan la obtención de esa respuesta.

La Inteligencia de Negocio (BI) es un término genérico que incluye las aplicaciones, la infraestructura y las herramientas, y las mejores prácticas que permiten el acceso y el análisis de la información para mejorar y optimizar las decisiones y rendimiento. (Gardner, 2018, párr. 1)

2.2.2.5 *Machine Learning*

El aprendizaje de máquina, aprendizaje automático o *Machine Learning* es una disciplina científica del ámbito de la inteligencia artificial que crea sistemas que aprenden automáticamente. Pallares (2014) afirma al respecto:

> Machine Learning puede ser ampliamente definida como métodos computacionales que usan la experiencia para mejorar el desempeño de las predicciones, logrando ser estas más precisas. Cuando nos referimos a experiencias hablamos específicamente de la información histórica recolectada que se utiliza para los procesos de entrenamiento. (párr. 7)

Relacionado al concepto anterior, en este proyecto se empleará esta disciplina para el análisis de datos, teniendo como referencia la información de los clientes, su perfil y comportamiento transaccional para proveer de material al modelo propuesto en su proceso de aprendizaje, con el

fin de obtener información precisa de aquellos movimientos atípicos que generen alertas ante posibles fraudes.

2.2.2.6 *Deep Learning*

El Deep Learning representa un acercamiento más íntimo al modo de funcionamiento del sistema nervioso humano. Nuestro encéfalo tiene una microarquitectura de gran complejidad, en la que se han descubierto núcleos y áreas diferenciados cuyas redes de neuronas están especializadas para realizar tareas específicas.

Viscaya (2018) menciona: "El Deep Learning permite a los modelos computacionales que están compuestos de múltiples capas de procesamiento, aprender representaciones de datos con diferentes niveles de abstracción" (p.20); también el mismo autor en su documento amplia el concepto, el cual lo define como:

> Un enfoque de la Inteligencia Artificial, un tipo de aprendizaje automático que alcanza gran potencia y flexibilidad mediante el aprendizaje de la representación del mundo, a través de conceptos jerárquicamente anidados. Se trata de formar conceptos complejos mediante la extracción y concatenación de conceptos muy simples. (p. 20)

Una representación visual del origen y estructura del Deep Learning se expresa en la siguiente figura:

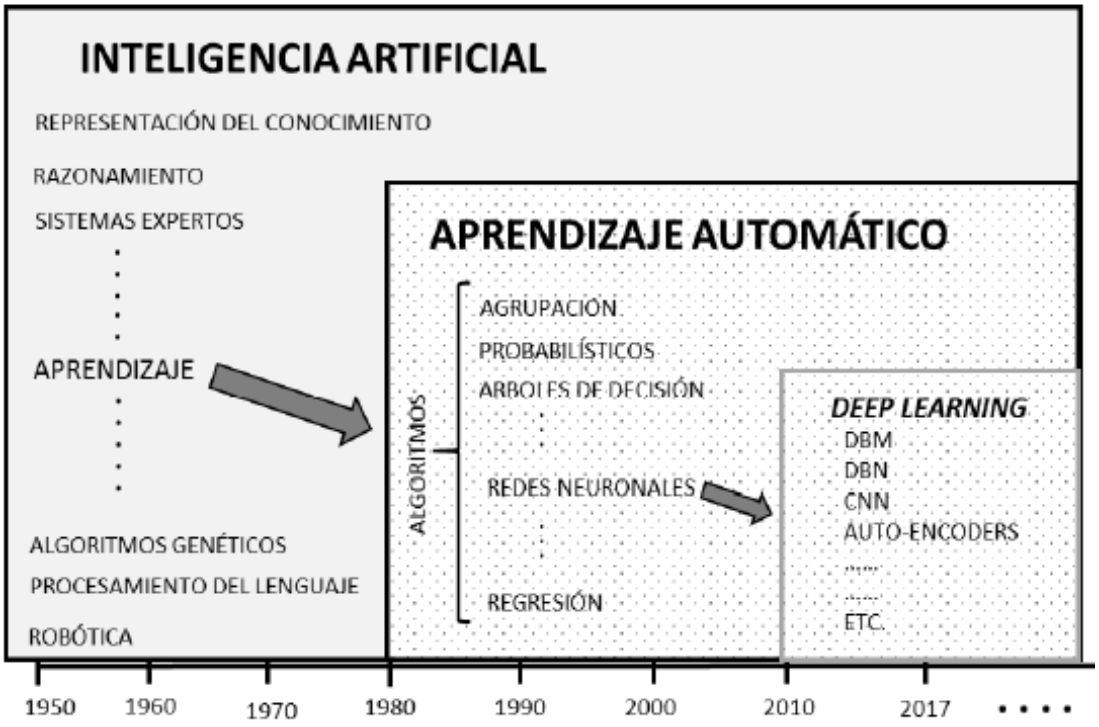


Figura 2: Ubicación del paradigma Deep Learning

Fuente: (Viscaya, 2018, p. 22)

CAPÍTULO 3:

MARCO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

3.1.1 Enfoque de la Investigación

Según lo plantea Roberto Hernández Sampieri, en su libro "*Metodología de la Investigación"* (2010) "El tipo de Investigación, independientemente del objeto al que se aplique, tiene como objetivo solucionar problemas. Además, describe el tipo de investigación como una especie de brújula en la que no se produce automáticamente el saber" (p. 4).

Para efectos de este proyecto, la investigación será: primeramente de tipo aplicada porque se dará respuestas a preguntas específicas en la resolución del problema, centrando en cómo se puede llevar a la práctica las teorías generales; y segundo, será de campo porque se resolverá una necesidad en un tiempo determinado, basado en la recopilación de datos en un ambiente natural en donde diferentes individuos serán la fuente de los datos a analizar.

La investigación aplicada recibe el nombre de **investigación práctica o empírica**, que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. Tanto del uso del conocimiento como de los resultados de investigación se obtiene una forma rigurosa, organizada y sistemática de conocer la realidad. (Vargas, 2009, pág. 5)

Con el fin de ampliar la idea de la investigación de campo para este proyecto (QuestionPro, 2018) menciona: "La investigación de campo es la recopilación de datos nuevos de fuentes primarias para un propósito específico. Es un método cualitativo de recolección de datos encaminado a comprender, observar e interactuar con las personas en su entorno natural" (párr.4).

Es importante resaltar que la idea fundamental de este tipo de investigación se refuerza en el análisis que se le dará a la información, conociendo la estructura de la seguridad de la información

que maneja la entidad financiera, sus reglas de negocio y todos los módulos que permitan desarrollar y obtener los datos relevantes para el modelo de detección de fraudes.

En cuanto al enfoque de la investigación, este de carácter cuantitativo, Sampieri (2006) menciona: “El enfoque cuantitativo usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías” (p. 4).

La mención anterior respalda la metodología del proyecto, ya que esta se basa en la recolección numérica de los eventos maliciosos reportados por los diferentes canales electrónicos en perjuicio de clientes de la institución financiera.

3.2 FUENTES DE INFORMACIÓN

Las fuentes de información de donde se obtendrá en sustento teórico y práctico de este proyecto se describen a continuación:

3.2.1 Fuentes Primarias

Según el autor Hernández Sampieri, “Las referencias o fuentes primarias proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes.” (Hernández Sampieri, 2010, pág. 53).

Como parte de las fuentes primarias que se utilizaran en esta propuesta se utilizan los reportes y eventos generados por los departamentos del Banco Nacional de Costa Rica relacionados a la gestión de fraude financiero y seguridad de la información, los cuales brindarán información esencial que facilitará la investigación; además de documentación interna de la Institución como

manuales de procedimiento, Metodologías internas, revistas y documentación publicada en la Intranet del Banco Nacional de Costa Rica.

3.2.2 Fuentes Segundarias

Entre algunas de las fuentes secundarias son investigaciones con contenido similar al que se plantea en esta propuesta, libros y resúmenes con contenido relacionado al tema, entrevistas a las partes interesadas del proyecto y análisis de normativa vigente que rige para la Institución Financiera.

Cabe mencionar que el criterio de los colaboradores que se relacionan día con día con la problemática de fraudes será parte fundamental de la investigación, aunque existen una serie de procedimientos y políticas definidas en la institución, la experiencia en el campo y los eventos que se presenten durante el desarrollo del proyecto reforzara el contenido de este.

3.2.3 Sujetos de Información

Los sujetos de la información que contribuirán a la obtención de información fiable para el desarrollo del proyecto son los siguientes.

Tabla 1*: Sujetos de la Información*

Puesto Laboral	Profesión	Experiencia	Relación con el Proyecto
Director de Seguridad Informática	Ingeniería	Dirección de Proyectos Institucionales	Dirección de Proyectos - Toma de Decisiones
Jefe Seguridad Bancaria	Ingeniería	Análisis de Datos	Modelo de Gestión - Reglas del Negocio

Jefe Plataforma de Servicios	Administrador	Gestión de Servicios Financieros	Consultor de Servicios y Procedimientos
Especialista Informático	Ingeniería	Análisis Base de Datos y modelos relacionales	Apoyo Diseño Propuestas
Técnico en Criminalística	Técnico Especializado	Investigación y análisis de timos o fraudes financieros	Apoyo Diseño Propuestas

Fuente: Elaboración Propia

La identificación de las necesidades se inició con el diagnóstico realizado al Banco Nacional de Costa Rica, el cual debido a los resultados obtenidos requiere de una solución informática en cuanto al tema de fraude.

3.3 TÉCNICAS Y HERRAMIENTAS DE RECOLECCIÓN DE DATOS

Según Dennis Chávez de Paz, en el 2009, en su libro *Conceptos y Técnicas de Recolección de Datos en una Investigación*, menciona que: "Cuando hablamos de recolección de datos nos referimos a información empírica abstraída en conceptos. La recolección de datos tiene que hacer con el concepto de medición, proceso mediante el cual se obtiene el dato, valor, o respuesta para la variable que se investiga" (p. 1).

Las técnicas y herramientas de recolección de datos son una pieza fundamental en el desarrollo y análisis del proyecto. La forma en la que se obtendrán los insumos para ser analizados, la calidad de esa información y todos aquellos detalles que hagan referencia a la situación actual del sector financiero en temas de fraude informático, permitirán brindar un panorama claro de las debilidades que se atacarán, las cuales deberán ser fortalecidas con las reglas de negocio del banco.

Conocer el flujo de recolección de los datos facilita la interpretación de esta etapa, como se muestra a en la siguiente página.

Figura 3: Recolección de Datos
Fuente: (Mora, 2010)

En la propuesta para el desarrollo del modelo planteado en este proyecto se utilizan algunas herramientas con el fin de recolectar la información necesaria para la ejecución y diseño, seguidamente se detallan aquellas que posiblemente se aplicarán:

3.3.1 Entrevista

Es importante conocer los diferentes escenarios que presenta el Banco Nacional de Costa Rica cuando es involucrado en un fraude informático por medio de sus canales financieros, ya sean electrónicos o presenciales. Por esta razón, es importante conocer el criterio de los encargados de cada sección junto con los datos correspondientes para su respaldo.

Se puede decir que la entrevista no se considera una conversación normal, sino más bien una formal, con una intencionalidad, que lleva implícitos unos objetivos en específico englobados en

una investigación concreta. Las entrevistas se aplicarán en la etapa de la obtención de la información al equipo de expertos detallados en la sección de Sujetos de la Investigación.

Se pretende para efectos del desarrollo de esta etapa, realizar un formulario el cual contendrá preguntas y escenarios claves que amplíen la situación actual en cuanto a los eventos de fraude informático y como las entidades financieras resuelven mediante sus procedimientos estos actos delictivos.

3.3.2 Observación

La observación es una técnica de análisis de hechos durante la cual el analista participa y actúa como espectador de las actividades llevadas a cabo por una persona para conocer mejor su sistema. El propósito de la observación es múltiple, permite al analista determinar qué se está haciendo, cómo se está haciendo, quién lo hace, cuándo se lleva a cabo, cuánto tiempo toma, dónde se hace y por qué se hace.

Es importante para este proyecto, conocer las formas en que se realizan las gestiones o bien la forma en que se registran los eventos maliciosos, determinar cómo se ejecutan los procedimientos y cómo son canalizados los reportes hacia los diferentes departamentos para su solución, con el fin de verificar si se están cumpliendo las normativas y políticas del Banco Nacional de Costa Rica de acuerdo con los parámetros establecidos por la administración y por la Dirección General de Tecnología.

Se pretende, para el desarrollo de esta etapa, crear un *check list* el cual contendrá una rúbrica básica para el registro del proceso manual cuando se detecta un fraude informático, esto se cotejará contra los procedimientos establecidos en temas de seguridad y seguridad de la información.

3.3.3 Diagrama de Flujo

Rivero (2008) menciona que: Es una representación pictórica de los pasos en proceso. Útil para determinar cómo funciona realmente el proceso para producir un resultado. El resultado puede ser un producto, un servicio, información o una combinación de los tres. Al examinar como los diferentes pasos de un proceso se relacionan entre sí, se puede descubrir con frecuencia las fuentes de problemas potenciales (p.70)

El diagrama de flujo podría ser una de las posibles herramientas en la recolección de datos para el desarrollo de este proyecto, la forma que se emplea y la estructura que lo constituye son una pieza importante para conocer los procesos que intervienen en la gestión y tramitación de un fraude informático.

Existe una metodología que se debe seguir en la aplicación de un diagrama de flujo, los cuales se mencionan a continuación:

- Propósito;
- Determinar el nivel de detalle requerido;
- Definir los limite;
- Utilizar los símbolos apropiados;
- Hacer preguntas: para cada input;
- Documentar;

- Completar: finalización de resultados;
- Revisión: inputs y outputs;
- Determinar oportunidades.

3.4 VARIABLES

3.4.1 Definición de Perfil y Comportamiento Transaccional

El perfil y comportamiento transaccional es la identidad, trazabilidad y operativa que tiene un cliente en el sistema bancario, esto le permite tener rangos o parámetros para poder gestionar sus trámites; además le abre las puertas a diferentes productos financieros que le ayuden a fortalecer su economía y a facilitar su entorno determinando su actividad comercial, de manera que cualquier movimiento inusual o atípico puede ser identificado por la institución financiera en un momento dado.

3.4.2 Definición de Detección de Fraudes

El fraude tiene muchos puntos en su estructura y conceptualización, sin embargo, la detección lo hace ver más complejo, ya que existen una serie de variables que a nivel práctico son imposibles de eliminar; estas variables se pueden determinar desde un enfoque cualitativo, siendo los clientes o usuarios vulnerables a miles de situaciones generadas por los actos delictivos de los estafadores, probando perjuicios económicos.

Para efectos de este proyecto la detección del fraude se puede definir como la anticipación de la materialización del evento malicioso mediante los canales financieros ofrecidos por el sistema bancario, ya sean presenciales o electrónicos.

3.4.3 Definición de Sistema Bancario

El sistema bancario es toda la red financiera que brinda servicios a los usuarios para el desarrollo y administración de su economía. Está compuesto por una serie de estructuras organizacionales y por diversas políticas internas de carácter privado y público. Y, además, es importante mencionar que existen normas internacionales que regulan las entidades financieras y además vienen a apoyar también las leyes contra delitos informáticos vigentes en el país.

En esta investigación nos referimos al sistema bancario como a la red de canales electrónicos ligados a cada usuario o cliente asociados a los servicios financieros que posee. En la siguiente tabla se hace entendible la relación de cada variable con cada objetivo planteado para el proyecto.

Tabla 2: *Variables de Investigación*

Objetivos Específicos	Variables Asociadas	Descripción
Identificar las principales vulnerabilidades presentadas por los usuarios ante un fraude en función de los servicios en línea o presenciales que utiliza.	Perfil y Comportamiento Transaccional	Mostrar la trazabilidad que mantiene un cliente con relación a los servicios financieros que maneja.
Justificar el proceso de detección de fraudes que se emplea en una entidad financiera enfocado en la aplicación de entrevistas en las plataformas de servicios.	Detección de Fraudes / Reglas del Negocio	Permite analizar los métodos utilizados por otras entidades financieras para la detección de fraudes, además de las políticas o reglas de negocio relacionadas a TI.

Valorar el perfil de los clientes y su comportamiento transaccional brindando criterios de análisis relacionados a los métodos de clasificación de la entidad financiera como segmentación, actividad económica e información bancaria.	Perfil y Comportamiento Transaccional / Eventos inusuales	Mostrar los movimientos efectuados por los usuarios, que cumplan con los perfiles asignados a su vinculación con la entidad financiera.
Establecer un cronograma de supervisión periódica que muestre indicadores de mejora en todas las áreas expuestas a eventos maliciosos por medio de experiencias.	Sistema Bancario / Monitoreo y Mejora Continua	Implementar un FODA al modelo con el fin de mantenerlo actualizado ante posibles eventos malicioso.

Fuente: Autoría Propia.

3.5 DISEÑO DE LA IVESTIGACIÓN

3.5.1 Fase de Identificación

En esta primera fase se pretende identificar los aspectos tanto teóricos como metodológicos para dar respuesta a cada objetivo definido en la investigación.

3.5.2 Fase de Revisión y Comparación

En este punto se quiere concentrar el proyecto en la revisión y comparación de los procedimientos, normativas y políticas que posee el Banco Nacional de Costa Rica contra otras estructuras del sector financiero tanto público como privado, con el fin de reforzar o bien considerar oportunidades de mejora.

3.5.3 Fase de Análisis y Aplicación del Teorema de I.A.

En esta fase se procede a analizar los perfiles de los clientes basados en su comportamiento y vinculación con el banco, además de su historial o récord financiero; seguidamente se aplicarán los teoremas de *Machine Learning* y *Deep Learning* enfocas en la I.A (Inteligencia Artificial) con el fin de extraer la información correspondiente, para la detección de fraudes cuando se presenten eventos inusuales o atípicos que no sean reportados o bien confirmados previamente con el cliente.

3.5.4 Fase de Monitoreo y Mejora continua

La actualización periódica del modelo de perfil y comportamiento transaccional y los resultados obtenidos en su desempeño, son trascendentales en esta fase; las reglas de negocio y el entorno cambiante de los sistemas informáticos requieren de un monitoreo constante, de tal manera que se puedan identificar aquellos eventos maliciosos que no hayan sido detectados previamente. Con esto se quiere conseguir que el modelo de perfil y comportamiento transaccional aprenda una información precisa y que de este modo brinde una solución que se adecue.

El resultado de este proceso se traduce en una mejora continua en donde el modelo mostrará, mediante indicadores, aquellos aspectos en donde deberá ser reforzado, lo que conlleva nuevamente a la fase de identificación.

3.6 MATRIZ DE COHERENCIA

Tabla 3: *Matriz de Coherencia*

Objetivo	Entregable	Fase	Métodos de recolección	Temas relacionados para el marco teórico
Identificar las principales vulnerabilidades presentadas por los usuarios ante un fraude en función de los servicios en línea o presenciales que utiliza.	Historias de usuarios	Fase 1	Observación y Entrevista	Modelo de Perfil / Comportamiento transaccional
Justificar el proceso de detección de fraudes que se emplea en una entidad financiera enfocado en la aplicación de entrevistas en las plataformas de servicios.	Informe de investigación	Fase 1 y Fase 2	Entrevista	Fraude / Fraude Informático y Financiero
Valorar el perfil de los clientes y su comportamiento transaccional brindando criterios de análisis relacionados a los métodos de clasificación de la entidad financiera como segmentación, actividad económica e información bancaria.	Resultados de análisis BI (Business Intelligence)	Fase 3	Observación y Diagrama de Flujo	Comportamiento transaccional / (Business Intelligence)
Establecer una guía de supervisión periódica que muestre indicadores de mejora en todas las áreas expuestas a eventos maliciosos por medio de experiencias.	Cronograma de supervisión	Fase 4 y Fase 1	Observación	Inteligencia Artificial/Machine Learning

Fuente: Elaboración Propia

CAPÍTULO IV:

DIAGNÓSTICO

4.1 DESCRIPCÓN DE LA SITUACIÓN ACTUAL

Actualmente, el Banco Nacional de Costa Rica carece de un modelo estratégico que le permita la detección o prevención de los fraudes informáticos en relación con los perfiles y comportamientos transacciones que poseen sus clientes ante los diferentes servicios que brinda la institución.

El fundamento de gobernabilidad del Banco Nacional es sumamente complejo, y se comenzó a ejecutar por una serie de iniciativas que permitieron al Banco, en el 2017, poder tomar una serie de decisiones que se encaminaran a cambiar el panorama de ciertos productos que contenían un mayor riesgo. Este esfuerzo fue posible gracias a un involucramiento de varias aéreas con el fin de brindar un apoyo comprometido ante la problemática.

Según el análisis realizado, el susodicho banco tiene tres aspectos fundamentales en su estructura de prevención de fraudes: antes, durante y después. Estos puntos determinan el procedimiento de reacción que se debe seguir para la detección de un evento malicioso, sin embargo, existe una serie de deficiencias en estos aspectos, las cuales serán descritas *groso modo* con el fin de ampliar la situación actual.

4.1.1 Situación Actual: Seguridad de la Información

El Departamento de Seguridad de la Información del Banco Nacional de Costa Rica, en materia de gestión de análisis periódico, identifica una serie de indicadores que resumen la situación actual en el manejo de los casos de fraude y el seguimiento que se les da a estos eventos.

A continuación, se describen los principales indicadores:

- Falta de atención integral de los fraudes materializados; esto es, cuando en el proceso de seguimiento el fraude ya se efectuó pasa a un segundo plano, debido a que ya no hay mayor interés por solventar la situación del cliente.

- Falta de promesas de calidad en resolución de casos; los tiempos de respuesta son significativos los cuales rondan entre los 30 a 40 días, esto ocasiona una serie de situaciones incomodas a los afectados.

- No existe un área específica que se encargue de la intervención inmediata del fraude; en consecuencia, esto conlleva a listas de espera y niveles de priorización para la resolución de eventos. En muchos casos no se tiene claro el tipo de fraude o bien lo existe documentación de referencia.

- Duplicación de actividades; al no tener un área centralizada que administre los eventos, es común que cuando un cliente interpone un reclamo en una oficina determinada, tiempo después tenga que realizar la misma gestión en otra oficina porque la primera gestión no se procesó o nunca se envió a los encargados en ese momento de los tramites.

- Falta de divulgación, capacitación interna y simulacros de preparación ante el fraude; no existen lineamientos claros que sean evaluativos a cada cliente según su perfil financiero, además, existe un desconocimiento de procedimientos o señales de alerta ante intentos de fraude y el personal de servicios no tiene material inmediato para determinar si el cliente ha sido víctima.

- Ausencia de sistemas informáticos integrales a nivel corporativo; se evidencia en la carencia de un modelo que permite a la administración tener un panorama más claro de los eventos y como realizar una gestión para su atención.

- Esfuerzos aislados en la organización; al ser una problemática institucional existen varias dependencias que proponen iniciativas, sin embargo, estas iniciativas deben pasar por una serie de procesos que al final no se concretizan.

4.1.2 Situación Actual: Seguridad de la Información

Actualmente el Departamento de Seguridad Informática del Banco Nacional es el encargado de mantener una estandarización en temas de seguridad a las diferentes dependencias que tienen relación o aplican algún tipo de proceso en su operativa; estar actualizados con las mejores prácticas internacionales es parte fundamental de este departamento.

Hasta el momento, muchos de los esfuerzos implementados tienen como objetivo principal salvaguardar los intereses de la institución y por ende los intereses de los clientes, sin embargo, ante un aumento de servicios electrónicos la responsabilidad, en cuanto al correcto uso de los mismos, ha recaído en su mayoría en los clientes, razón por la cual esto se convierte en un tema sumamente complicado para el departamento de seguridad a la hora buscar medidas informativas y de prevención con el fin de disminuir las vulnerabilidades a las que están expuestos los usuarios.

En vista de la situación expuesta, la mayor necesidad de esta dependencia es contar con un modelo administrativo que simplifique y unifique en un solo lugar todos aquellos conceptos, procedimientos y reglas de negocio, en un ambiente de aprendizaje continuo.

4.1.3 Situación Actual: Sistema Financiero

Dentro del sistema bancario, muchas instituciones financieras comparten la necesidad de optar por un modelo de detección de fraudes para fortalecer su seguridad en los productos o servicios que brindan a sus clientes, inclusive se han visto expuestos a trámites legales en donde tienen que asumir cierta responsabilidad ante un evento delictivo, y en esto, el Banco Nacional no es una excepción.

Según La Teja (2017) periódico de circulación nacional: "un pensionado farmacéutico, demandó al BCR en el 2011 por haber sido víctima de fraude informático, el mismo en su demanda consideraba que la institución no contaba con las herramientas de seguridad necesarias en su página web, para proteger sus ahorros" (párr. 1-3). En esta demanda el usuario mencionaba que la página contaba con todas las especificaciones habituales, es decir: logos, colores, solicitud de datos, entre otras características.

La licenciada Adriana Rojas, con relación a este caso, explicó qué: "en el momento que un cliente deposita su dinero en el Banco está confiando [en] que la empresa es segura y no se imagina que un error personal, ponga en riesgo el dinero de todo su trabajo. Por otro lado, los directivos del BCR dieron pruebas de que el actor facilitó información vital para que los ciberdelincuentes accedieran a su cuenta y extrajeran un monto cercano a los $2.000" (párr. 3-5)

En este caso, al parecer no hubo mayores pérdidas para el banco puesto que el afectado solicitaba una total indemnización por parte del banco y asumiera las costas del proceso; no obstante, el Tribunal de primera instancia acogió parcialmente y dispuso que debía reconocer únicamente el 50 por ciento del daño sufrido.

La problemática es que, aunque en este caso no hubo una perdida monetaria significativa para el BCR, si hay una afectación para la confiabilidad de los usuarios. Especialmente, como en el

caso anterior, si se evidencia la falta de algún mecanismo que pudiera haber evitado o prevenido el acto delictivo al que fue víctima estuvo expuesto. Por otro lado, se debe tomar en cuenta que, mediante los *mass media* se puede llegar a poner en duda la reputación de la banca pública, de sus deficiencias en controles y temas de seguridad informática. Pablo Rojas (2014), del sitio web crhoy.com, afirma que:

> Los delitos informáticos son más frecuentes de lo que se cree; constantemente el país sufre de ataques cibernéticos a instituciones públicas, servidores importantes y sitios de gobierno. Es por este tipo de razones que los costarricenses deberían ser más cuidadosos y alimentar esa costumbre de verificar los sitios, cuidar sus claves y evitar abrir correos desconocidos, así lo indica el señor Gabriel Macaya, director de la Academia Nacional de Ciencias. (párr. 4)

Es vital que todas las instituciones públicas y privadas posean un departamento de seguridad, orientado a la seguridad de los sistemas y a los servicios y políticas tecnológicas que respondan ante eventos maliciosos, con el fin de proteger su infraestructura y los intereses de los clientes. En relación con esto, según el Banco Central de Costa Rica (BCCR) (2017):

> [Se] alertó al público en general sobre el aumento de intentos de estafa tanto por la vía telefónica como por correo electrónico, en los cuales, [los estafadores] se hacen pasar por supuestos funcionarios de la Institución, con el fin de obtener datos como números de cuentas bancarias y claves de acceso (…) En los últimos seis meses, el BCCR ha recibido 107 denuncias de intento de estafa, en las que al menos en dos ocasiones se

> consumó el delito, de acuerdo con el relato de los denunciantes. Si bien durante todo el año se han reportado casos, en agosto y las dos primeras semanas de setiembre las denuncias aumentaron de manera considerable, pues acumulan el 60% de los casos conocidos por la entidad. (párr. 1-3)

Ahora, en cuanto a los métodos de estafa, uno de los eventos delictivos más comunes efectuado por los delincuentes está relacionado al cambio de formato de cuentas cliente de 17 dígitos numéricos hacia el estándar IBAN (International Account Number), el cual consta de 22 dígitos alfanuméricos e identifica cuentas de fondos tanto a nivel nacional como internacional; básicamente el delincuente contacta a una persona por medio de una llamada telefónica, el mismo se hace pasar por un funcionario de una entidad bancaria y solicita al cliente una serie de datos para posteriormente cambiar sus claves y sustraer su dinero, entre otras gestiones fraudulentas.

Siguiendo el mismo comunicado del Banco Central, se han realizado varios esfuerzos con diferentes entidades financieras sobre la importancia de comunicar a sus clientes, que la institución ni ninguna otra entidad del sector financiero llaman a sus clientes o envían correos electrónicos para solicitar datos personales (números de cuentas, claves de acceso o *passwords*, datos de tarjetas y otros) por supuestos cambios o actualizaciones de las cuentas bancarias.

Los estafadores están utilizando la técnica de suplantación de la dirección de correo electrónico o *MailSpoofing*, en función, cuando alguien envía un correo donde el campo del remitente (From: o De:) es falso, de forma que se hace creer que el correo ha sido enviado por una persona o entidad que se quiere suplantar, en este caso al Banco Central de Costa Rica. En los casos detectados por la Institución, los estafadores hacen creer a la persona que el correo fue enviado desde la dirección de correo electrónico info@bccr.fi.cr (Banco Central de Costa Rica, 2017, párr. 4).

4.2 RECOLECCIÓN DE DATOS

Dentro del análisis de la información, surge la necesidad de aplicar una serie de entrevistas al personal de seguridad de la información y al personal de seguridad bancaria, ambas dependencias del Banco Nacional, esto con el fin de completar la etapa de diagnóstico operativo y diagnostico técnico.

Las preguntas realizadas al personal se enfocan directamente en la gestión y administración de la seguridad informática, tomando como tema principal los timos o fraudes informáticos. El criterio de los funcionarios y la experiencia en el campo proveen de un contenido sumamente enriquecedor al desarrollo de esta etapa.

4.2.1 Entrevistas Diagnóstico Operativo y Técnico

Se realizan cinco entrevistas, de las cuales tres son aplicadas al personal de Seguridad Bancaria (ver Anexo 1) y dos al personal de Seguridad Informática del Banco Nacional (ver Anexo 2).

Se presentan los resultados a continuación:

Entrevista

Dirección de Seguridad Bancaria.

Banco Nacional de Costa Rica.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A) Explicación breve de objetivo general y objetivos específicos.

1. Para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.

Respuesta #1

Tengo amplia experiencia en temas de seguridad, cuento con más de 20 años laborando para el Banco nacional. Anteriormente trabajé para el Organismo de Investigación Judicial (OIJ) como investigador y oficial de campo. Actualmente desempeño el cargo de jefe de seguridad en la Dirección de Seguridad del Banco Nacional y como jefe de seguridad velo por todos los aspectos administrativos relacionados a las diferentes situaciones que se presenten en las oficinas en temas de fraudes, estafas, asaltos, entre otros eventos delictivos.

Respuesta #2

Tengo más de 14 años de experiencia en temas de seguridad en el Banco Nacional [desde que] el tema de los fraudes no se conocía o era muy nuevo en entidades financieras. De profesión, soy licenciado en ingeniería en sistemas y desde junio del 2017 estoy realizando mis funciones en la Dirección de Seguridad y soy el único experto en análisis de reclamos administrativos mediante internet *banking.*

Respuesta #3

Tengo 16 años de experiencia a nivel de seguridad bancaria, soy graduado en criminalística. Las funciones que realizo acá en la Dirección de Seguridad tratan de temas de asistencia a la parte investigativa sobre cualquier tipo de fraude que se pueda llevar acabo o donde exista una noticia de crimines expuesta por parte de algún cliente, es ahí donde nosotros llegamos a actuar. Dentro de los tipos de fraude que se logran establecer serian fraudes con cheques, timos de depósito, ventas por internet con el fin de obtener información sensible para conocer datos del cliente y posteriormente realizar una estafa y lo que está más en boga, son los fraudes mediante servicios electrónicos o fraudes informáticos.

2. ¿Cómo se realiza actualmente el proceso de gestión del fraude materializado (servicios digitales)?

Respuesta #1

El cliente primero debe interponer un reclamo administrativo en cualquiera de los siguientes canales: centro de llamadas, Contraloría de Servicios o en la red de oficinas del Banco Nacional. Posteriormente, debe presentar una denuncia formal ante el OIJ, seguidamente traer toda la documentación a las oficinas del banco para que sea recibida por el personal correspondiente. Luego, la información será analizada con el fin de determinar la veracidad del fraude y seguir con procedimientos establecidos por la institución y las leyes judiciales del país.

Respuesta #2

Desde el 2005 el Banco Nacional ha venido gestionando todas las modalidades de eventos delictivos en torno a sus servicios electrónicos, algunas de las cuales han sido simples pero funcionales para su época, en otras palabras, han logrado su cometido. En el 2008 implementamos el *token* celular vino a brindar una mayor seguridad en las transacciones, sin embargo, los delincuentes mejoraron su operativa y continuaron "timando" a los clientes, razón por la cual, buscando una mejora continua en el 2009 se implementa el *token* llavero y el teclado virtual, entonces, gracias a ese esfuerzo del 2010 al 2015 no se reportaron timos por medio de internet *banking*.

Para el 2016 se empiezan a detectar casos a un nivel delictivo mayor, los delincuentes copiaban los sitios web del banco y mediante buscadores, utilizando enlaces pagados, guiaban a los clientes a páginas falsas. Definitivamente el grado de programación era diferente, se conocía qué se estaba haciendo y cómo se estaba haciendo.

Luego empezaron a utilizar las llamadas telefónicas, método efectivo hasta la fecha, ya que el concepto de "timo" adquiere un giro considerable y da paso aparición de un fenómeno llamado **ingeniería social**. Entonces, nuestra función en cuanto a gestión de fraudes actualmente ha girado en torno a prevenir esta forma de adquisición de la información, mediante diferentes métodos de comunicación para tratar de informar a los clientes. Si el evento ya fue materializado, pues se realiza el proceso correspondiente a los lineamientos de la institución.

Respuesta #3

Se puede hacer de dos formas, que el cliente llame y avise a nuestro centro de contacto o que se apersone a una oficina bancaria, también puede suceder que el afectado no realice el reclamo en el banco, más sin embargo lo realiza ante el OIJ. Cuando el cliente realiza la gestión mediante el centro de contacto, el personal se encarga de deshabilitar todos aquellos servicios que estén ligados electrónicamente a los principales productos del cliente los cuales puedan poner en peligro su capital; finalizado este proceso el cliente deberá apersonarse a una agencia del banco a continuar con el proceso administrativo correspondiente. Si el cliente se presenta al banco directamente, será el plataformista quien se encargue de realizar la gestión y remitirnos el caso a nosotros una vez concluida la etapa de desafiliación de servicios.

Si el cliente realiza el reclamo ante el OIJ, será este organismo quien notifique al banco que un cliente el cual mantiene relación comercial con la institución presenta un posible fraude y con base a esa información nuestro departamento se encargará de realizar el debido proceso; es importante mencionar que para las gestiones anteriores siempre se debe identificar el tipo de fraude para poder canalizar la investigación de la mejor forma posible.

3. ¿Cuáles son las dificultades en ese proceso actualmente?

Respuesta #1

Básicamente las principales dificultades de este proceso se resumen en la revisión de la información en las distintas bases de datos. La información que se requiere para la investigación no está recopilada en una sola herramienta, lo que ocasiona atrasos en la creación de reportes. Por otra parte, el recurso humano a pesar de que cuenta con herramientas individuales, no es el suficiente como para hacerle frente a la cantidad de casos que se reciben en el departamento, presentándose nuevamente la misma problemática en cuanto a los tiempos de espera.

Respuesta #2

Definitivamente la ingeniería social que se le aplica a los clientes, ya que es lo más utilizado y el principal motivo de reclamos recibidos en nuestra dependencia. A pesar del esfuerzo realizado, el cliente sigue suministrando sus datos y su información bancaria ocasionando un reproceso en nuestras gestiones.

Respuesta #3

Muchas veces sucede que no hay un pronto alcance a la información, ya que el cliente cuando llama o llega al banco no es muy claro con lo que está solicitando, entonces el personal del banco debe extenderse en entrevistar para definir realmente cual es la situación del cliente y proceder con los bloqueos correspondientes. Para la empresa es sumamente importante la primera información, es vital para poder actuar con el fin de detener o prevenir un daño mayor al cliente.

4. ¿Qué procedimientos, políticas o reglamentos internos se aplican a cada etapa?

Respuesta #1

Bueno, se aplican todos los procedimientos y políticas establecidas en el mapa de procesos, sección que se encuentra en la intranet del Banco Nacional. Estos procedimientos brindan instrucciones técnicas para la gestión y atención de los diferentes eventos que correspondan a la Dirección de Seguridad.

Respuesta #2

La Contraloría de Servicios posee un procedimiento establecido por el banco, en el cual dicta los pasos a seguir cuando un cliente sufre de algún evento que preliminarmente se catalogue como fraude. El cliente debe presentar un reclamo administrativo, previo una denuncia ante el OIJ, adjuntar cierta información personal y esperar a que la gestión sea investigada por nuestra dependencia.

Respuesta #3

Para los funcionarios existe una matriz establecida para el protocolo de atención en caso de fraudes, ya sea por canales electrónicos, transferencias, etc., ya está parametrizado lo que tiene que hacer, cuáles son el a, b, c de lo que tiene qué hacer. Esta información se ubica en la intranet, en el mapa de proceso, completamente público para el funcionario y a las jefaturas para que lo tengan presente en sus oficinas ante cualquier situación.

Ahora bien, si existiera alguna situación atípica, sin ningún problema pueden llamar a nuestra dirección y con gusto podemos guiarlos o asesorarlos de la mejor forma posible para que puedan atender y gestionar la necesidad del cliente, máxime que algunos de ellos no tienen un solo servicio o una sola cuenta, sino que tienen diferentes productos con la institución y es importante determinar cuáles han sido afectados y cuáles deben bloquearse temporalmente.

5. **¿Se aplican correcta y linealmente los procedimientos, políticas o reglamentos internos?**

Respuesta #1

Es importante considerar que todos los casos que nosotros recibimos en el departamento por más simples que sean deben llevar un orden y un avance en cada etapa para que sea congruente con los procedimientos establecidos por la institución. No podemos omitir detalles debido a que estos casos pueden ser solicitados por dependencias judiciales o auditorías externas e internas.

Respuesta #2

Totalmente, cada proceso es vital. Debemos estar conscientes de que la imagen del banco y la forma en que resuelva los casos que recibe son las principales fortalezas que se tienen, el fin es brindar seguridad a sus clientes en el uso de los diferentes canales electrónicos.

Respuesta #3

Sí se aplican, pero siento que no a cabalidad tal vez porque falta un poco de *expertise* por parte del funcionario sumado a que el cliente, como lo mencioné anteriormente, no es muy claro, entonces se entra en un proceso de adivinar incluso la gestión que requiere el cliente. Para disminuir estas discrepancias, lo primero que se tiene que realizar y lo que nosotros le indicamos primero al funcionario es sacar al cliente de Internet Banking y BN Móvil, con el fin de cerrar portillos lo antes posible.

6. **¿Cómo debería ser la operativa según su opinión y experiencia en el proceso?**

Respuesta #1

Debería ser más expedita, que podamos procesar la información con mayor facilidad, simplificando tramites y tiempos de espera. Acceso a sistemas de información los cuales hoy en día son administrados en otros departamentos y para solicitar información debemos interponer un requerimiento, evidentemente esto genera tiempos y atrasos en el proceso.

Respuesta #2

Cuando el cliente identifica que ha sido timado, la acción más rápida es llamar al banco, cuando esta llamada es atendida por el call center el ejecutivo debe identificar al cliente y posteriormente ir sistema por sistema bloqueando servicios, claro está, no todos los sistemas son administrados en el call center, razón por la cual una debilidad es precisamente que no existe un módulo centralizado de administración que brinde una respuesta rápida y precisa de los servicios que deben ser bloqueados para salvaguardar el patrimonio de los clientes. Es importante promover campañas informativas acerca de la ingeniería social aplicada a los clientes, no solo en Banco Nacional, sino en todo el sistema financiero nacional.

Respuesta #3

Deben existir cambios, el Banco Nacional no se puede quedar en una sola matriz o proceso, ya que el fraude va llegar a mutar y a ofender, entonces deben haber constantes modificaciones en este caso de cada una de las áreas expertas o involucradas de crear los sistemas o procesos de seguridad, de manera que estén en continua actualización, porque el fraude siempre será fraude pero la modalidad que se utiliza es la que será diferente, por ende, debemos estar enfocados en atacar esas modalidades y tratar de reducir con medios informativos la vulnerabilidad que en la que se encuentran los clientes.

7. ¿Con cuáles herramientas (infraestructura física o lógica, sistemas, aplicaciones) cuenta el departamento de seguridad para el registro de los fraudes?

Respuesta #3

Desde el punto de vista de sistemas contamos con herramientas como: el SFB, el cual es un sistema de consulta de movimientos y transacciones de las cuentas de los clientes; un portal integrado de servicios, que contiene información diversa de los clientes como por ejemplo datos personales, perfil financiero, productos o servicios asociados, entre otros; bases de datos de las transacciones, las cuales son administradas por el departamento de seguridad informática del banco y otra base de datos pero orientada un poco más hacia la información policial administrada directamente por nosotros, el equipo de la dirección de seguridad.

En cuanto a infraestructura física, contamos en todas las oficinas del país con un circuito cerrado de cámaras, las cuales poseen las características necesarias para identificar cualquier situación que se presente. Brindamos charlas a diferentes departamentos con el fin de capacitar al personal (ejecutivos de cuenta, plataforma de servicios, servicio al cliente, etc.) en temas de seguridad y que sean ellos mismos los que trasmitan recomendaciones a sus clientes en el uso correcto de sus cuentas, además de la información que el banco se encarga de comunicar en los diferentes medios o redes sociales.

Respuesta #2

El departamento cuenta con el equipo físico necesario para el desempeño de las funciones, máquinas de escritorio, impresoras multifuncionales, etc. Por otra parte, a nivel de software se tiene acceso a los diferentes sistemas operativos y de consultas; estas consultas son realizadas mediante scripts en SQL cuando se requiere extraer de alguna base de datos, en

fin, nuestra dependencia tiene acceso directo o indirecto a todos los sistemas que la institución tiene.

Respuesta #3

Partimos de que sabemos cómo operan los delincuentes, cómo llegan al cliente, la forma en la que aplican una ingeniería social a una población con mayor vulnerabilidad, cómo se aprovechan de situaciones sensibles para materializar el timo o fraude conociendo que carecen de esa malicia. Desde el punto de vista de nuestro departamento, tenemos herramientas de revisión, de verificación, de análisis que provee el banco como lo son: el SFB; archivo virtual; el sistema de tarjetas de visa; bases de datos de IB, las cuales son importantísimas; el sistema de video electrónico, el cual nos sirve como evidencia ante un proceso solicitado por el OIJ; tenemos también bases de datos de reconocimiento de personas, de manera que se puede hacer una identificación primaria para que posteriormente el OIJ realice la investigación de campo según corresponda.

8. ¿Considera que el equipo actual (colaboradores y recurso tecnológico) cumple con los objetivos y alcances del departamento?

Respuesta #1

En el departamento de seguridad contamos con un recurso humano conformado por profesionales en áreas como administración e ingeniería, sin embargo, para efecto de sus funciones han ampliado sus conocimientos en temas de seguridad e investigación, lo que se quiere decir es que han aprendido a desarrollar sus funciones, aunque sus profesiones no se relacionen, es un tema de aprendizaje constante y experiencia día a día.

Se cumple con los objetivos a pesar de las limitantes, pero no por el personal, sino por las herramientas que se utilizan para el desarrollo de las investigaciones, que es lo que comentábamos anteriormente. Sería de gran ayuda tener un sistema o una plataforma que nos facilite la operativa, y por qué no un modelo que reúna ciertos criterios de las demás herramientas y que simplifique las gestiones que realizamos.

Respuesta #2

Podemos decir que sí, personalmente considero que algunas herramientas no funcionan como deberían o como se desearía ya que no existe tanta accesibilidad, quiero decir que se tiene que rastrear la información en las bases de datos.

La institución actualmente debe hacer un esfuerzo con los sistemas ya que nunca se pensó, dentro de los requerimientos, solicitar módulos de reportaría que faciliten la búsqueda de información ante situaciones de auditoría, casas de investigación, entre otros.

El recurso humano siempre será importante y es necesario que el personal se pueda capacitar y que brinde ese soporte a los incidentes que se reciben día a día con el fin de disminuir los tiempos de espera dándole una mayor fluidez a las gestiones. Las oportunidades de mejora son pilares en nuestra gestión, debemos ir actualizando los procesos, ir adelante y concientizar a los clientes sobre el uso de los servicios electrónicos.

Respuesta #3

Definitivamente considero que somos pocos, en relación con la gran cantidad de casos que ingresan por los diferentes canales de recolección de incidentes; el uso tecnológico es un factor, es fuerte, pero se necesitan más herramientas a la mano. Debemos acudir a varios departamentos para solicitar la información, esto evidentemente genera atrasos en los tiempos de respuesta.

La ausencia de un módulo que reúna todas las herramientas en un solo acceso en donde podamos obtener los insumos que requerimos para las investigaciones, sería de las mejoras que sugeriría, esto con el fin de no depender de otros departamentos y solventar los casos a la mayor brevedad posible.

El cliente tiene una gran responsabilidad y peca al no tomar esa responsabilidad como debe ser, no informarse, no entender de manera clara la información que se le brinda o hacer caso omiso a esa información, básicamente se define como una ausencia de cultura en términos de seguridad y el banco, como ente proveedor de servicios, debe esforzarse por ser más agresivo, si se puede llamar de esa manera, en comunicarle a los clientes las consecuencias que se pueden tener en suministrar a un tercero datos sensibles relacionados a productos financieros. Al final es un trabajo en conjunto de ambas partes para que el cliente haga conciencia de la forma en que utiliza los servicios y que el banco le brinde actualizadamente mecanismos confiables e información oportuna; aplicando esto no solo para Banco Nacional sino para todas las entidades financieras.

9. ¿Qué mejoras sugeriría usted para ambas áreas?

Respuesta #1

Definitivamente mayor recurso humano para hacerle frente de forma más rápida a los eventos que se reciben en el departamento. Como lo hemos venido conversando, una plataforma en donde podamos encontrar unificada toda la información que necesitamos o bien un modelo que simplifique la operativa.

Respuesta #2

Responde en la pregunta número 8.

Respuesta #3

Responde en la pregunta número 8.

Entrevista

Dirección de Seguridad Informática.

Banco Nacional de Costa Rica.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A) Explicación breve del objetivo general y de los objetivos específicos.

1. Para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.

Respuesta #1

Tengo 33 años de servir en el Banco Nacional, de los cuales los últimos 27 los he desarrollado en el departamento de tecnología en diferentes departamentos: desarrollo, aplicaciones, arquitectura, y actualmente laboro como director de seguridad informática. Me corresponde llevar la administración general en temas de ciberseguridad del departamento.

Respuesta #2

Mi experiencia profesional ronda los 25 años en temas de seguridad, he sido consultor y conferencista internacional siempre en temas de seguridad, además durante aproximadamente 12 años fui perito para el Banco Nacional en estemas de fraude, han sido

varios años en función; tengo también varias certificaciones de ISACA y he pertenecido a grupos de esta organización.

2. ¿Cómo se realiza actualmente la administración de la parte de la seguridad informática?

Respuesta #1

Nosotros estamos orientados a ver temas de: detección; atención; resolución de incidentes de ciberseguridad; análisis y posibles amenazas; nuevos métodos y soluciones para la gestión de la ciberseguridad; y también nos encargamos de identificar y recomendar la adquisición de nuevas soluciones.

Respuesta #2

Tenemos un grupo de trabajo que se encarga de validar y verificar todos los controles en las áreas del banco en temas de seguridad, aplicativos como internet *banking*, canales electrónicos, aplicaciones, etc. Además, damos seguimiento a plataforma, cajas, servicios al cliente, cajeros automáticos, es decir, es nuestra función que todos aquellos medios electrónicos se estén ejecutando acorde a las mejores prácticas.

3. ¿Cuáles debilidades o dificultadas puede determinar en esa administración?

Respuesta #1

Los retos más importantes que deben enfrentar los departamentos de ciberseguridad y no solo el Banco Nacional sino todas las entidades financieras, giran en torno al gran volumen de transacciones que actualmente se están realizando por diferentes medios electrónicos, estos servicios son 24/7 y los clientes hacen un uso constante de ellos. A esto debemos

agregar que ahora las soluciones tecnológicas que ofrecen los bancos están basadas en infraestructuras híbridas, es decir, multiplataforma y también instaladas en diferentes *Data Center*. Todo esto ha captado la atención por parte de los departamentos de ciberseguridad, ya que surgen entornos más complejos debido al volumen transaccional que se está manejando.

Respuesta #2

Siempre se encontrarán oportunidades de mejora, los delincuentes pondrán en práctica nuevas formas de atacar y probar nuevos mecanismos, ya que tienen el tiempo necesario para efectuar y concretar el delito; en ese sentido es importante que nuestro departamento esté alerta ante esta situación y realizar las funciones de forma correcta. La mayor debilidad es no poder anticipar estos nuevos métodos, sin embargo, estamos en constante actualización acorde a las mejores prácticas de seguridad.

4. ¿Qué procedimientos o gestiones aplican ustedes día con día en la dirección de seguridad informática?

Respuesta #1

Existe toda una estructura de gobernanza en temas de seguridad para el conglomerado en donde destaca que la Junta Directiva del Banco Nacional es el máximo órgano en entender, dar seguimiento y gestionar todos los temas de seguridad y de riesgo. También existen diferentes comités de apoyo que atienden a la Junta Directiva, los cuales reciben retroalimentación técnica de las diferentes dependencias relacionadas a temas de seguridad y de riesgo operativo. Todo esto está respaldado en una base documental en donde existen políticas institucionales sobre temas de seguridad y ciberseguridad, normativas alineadas con

la ISO 27001 para todo el tema de controles, políticas y procedimientos específicos para las dependencias que tienen relación directa con temas de seguridad

Esta base documental está disponible en la intranet para todas las dependencias del banco, se trata de un acceso directo a las normativas y políticas de seguridad y, muy importante, un sitio para el ingreso de eventos e incidentes de seguridad.

Respuesta #2

Se realiza una revisión constante de vulnerabilidades, validando que las mejores prácticas estén implementadas en los sistemas, además tenemos procedimientos que nos permiten tener una guía para validar las normativas y convertirlo en políticas para las diferentes áreas respectivas. También tenemos procedimientos que nos permiten primero, ayudar a los compañeros a detectar situaciones que no sean normales o fuera de las prácticas comunes, principalmente en el área de producción y segundo, guiarlos según las normas recomendadas.

Parte de los procesos que estamos siguiendo en temas de certificación de calidad es que toda la documentación que utilizamos para este asesoramiento esté al alcance de los funcionarios de la institución, siendo las áreas más prioritarias el departamento de cajas, plataforma, ejecutivos de cuenta y jefaturas. Esto nos permite tener una mejora continua ya que los procesos son sometidos a una evaluación constante.

5. **¿Se aplican correcta y linealmente los procedimientos, políticas o reglamentos internos?**

Respuesta #1

Totalmente, se debe señalar que somos regidos u observados por entes reguladores internos y externos.

Respuesta #2

Eso es precisamente lo que se busca, que los procedimientos estandaricen la forma de operación.

6. ¿Cómo debería ser la operativa según su opinión y experiencia en el proceso, buscando que sea más expedita?

Respuesta #1

Existen 3 aspectos importantes que debemos seguir desarrollando en el banco:

- La cultura de seguridad, entender que todos en el conglomerado tenemos una responsabilidad en temas de seguridad.

- Trabajar fuertemente temas de automatización, como hemos hablado, el volumen transaccional que está manejando la institución es enorme, eso no se puede hacer por métodos anuales o herramientas de uso cotidiano, sino requerimos herramientas que procesen en tiempo real la información, definir o establecer tendencias, visualizar desviaciones, para luego tomar de decisiones oportunas.

- Reforzar las estructuras operativas, tanto a nivel de cantidad como de preparación y obviamente de herramienta.

Respuesta #2

La inteligencia artificial es una tecnología que vendría a solucionar muchos de los procesos que actualmente requieren una gestión más lenta, un sistema o modelo: que brinde estadísticas de manera que los eventos sean identificados a nivel de transaccionalidad del cliente y que sean más analíticos y durante 24/7; que logre determinar comportamientos y acciones que puedan estar sujetas a intereses específicos con el fin de considerar que estén fuera de rangos de usabilidad y periodicidad para evitar pérdidas de patrimonio de los clientes.

7. ¿Con cuáles herramientas cuenta el departamento de seguridad informática para la administración?

Respuesta #1

El Banco toma muy enserio los temas de seguridad y desde hace bastante tiempo invierte cantidades importantes de recursos para contar con las herramientas que establezcan la mejores prácticas pero también se han venido incorporando las herramientas que requieren las demandas del negocio y las tendencias a nivel de amenazas y de buenas prácticas, el banco cuenta con herramientas tradicionales como: *IPS; fireware; WAF; SOCK*; herramientas de monitoreo, de análisis de correos, de análisis de control de navegación, etc., lo que se considera como tradicional. También se han hecho inversiones en herramientas con aprendizaje de máquina y AI para lo que es análisis de datos de tal forma que toda la información esté dirigida tanto a reforzar la prevención y detección de fraudes como a la contención de incidentes.

Respuesta #2

El Departamento de Seguridad Informática guía a todas las áreas operativas, no está relacionado directamente con la operativa. Las asesoramos en el desarrollo de sus herramientas y mejora continua, por ende, se cuenta con un personal que se encarga de estas gestiones, por

otra parte, cualquier modelo o sistema que ayude a fortalecer la administración de la seguridad será bienvenido.

8. ¿Considera que el equipo actual (colaboradores) cumplen con los objetivos y alcances del departamento?

Respuesta #1

La seguridad no es un destino es necesariamente un proceso y todas estas herramientas tienen que ser administradas día a día, actualizadas en todas sus configuraciones para que estén acorde a las nuevas amenazas y los nuevos vectores de ataque, por ende, se tiene que estar en una mejora continua para cumplir con los objetivos principales de la institución.

El tiempo es muy relativo, en este momento se puede tener todos los elementos o herramientas, pero en 60 segundos ya estarán desactualizados y se deberá hacer modificaciones buscando otra solución o mejorar lo que se tiene.

Respuesta #2

Es un tema de nunca acabar, cuántas personas se necesitan para determinada tarea. Proporcionalmente siempre se buscará alcanzar las mejores prácticas, el Banco Nacional ha buscado hacerlo, la mejor práctica actual relaciona la cantidad de inversión en tecnología con la inversión en seguridad. Contar con suficiente recurso humano siempre es importante, más si se quiere alcanzar un estándar internacional que está reconocido y para lo cual ya falta poco.

9. **¿Qué mejoras o recomendaciones sugeriría usted enfocándose en la responsabilidad que tiene el cliente, el Banco y las diferentes dependencias en temas de seguridad informática?**

Respuesta #1

La seguridad es un trabajo en equipo en donde el banco tiene una enorme responsabilidad como prestatario del servicio, pero donde también el accionar de los clientes internos y externos es factor críticos para éxito, esto implica que todos los clientes deben saber de seguridad, pero lo más importante que deben desarrollar sus labores y utilizar lo diferentes canales que tiene los bancos con suma prudencia y diligencia.

Todos los elementos de seguridad enfocados a los servicios están custodiados por los clientes, por ende, reiteramos que se deben de utilizar con mucha prudencia y una adecuada custodia, ya que en los últimos meses el principal medio utilizado por los delincuentes es la ingeniería social, por ende, se debe crear conciencia de que somos elementos esenciales dentro del esquema de seguridad.

Respuesta #2

Como lo hemos venido conversando, las nuevas tecnologías y el uso de la inteligencia artificial en un modelo que potencialice: la analítica del comportamiento transaccional de los clientes; el uso responsable de la información bancaria por parte de los usuarios en las plataformas digitales; el compromiso de cada uno de los funcionarios del banco para mantener un sentimiento tanto de responsabilidad como de mejora de procesos, es la recomendación que haría en toda la administración y operativa de seguridad informática.

4.2.2 Diagnóstico Operativo

Las entrevistas realizadas a los departamentos de seguridad bancaria y seguridad informática muestran conceptos muy similares en cuanto al proceso operativo de la gestión y atención del timo o fraude informático mediante canales electrónicos. Varios de los participantes determinaron que el correcto proceso de atención de un reclamo administrativo proveniente de un timo o fraude informático es vital para tomar las medidas subsiguientes para lograr detener el daño al cual está siendo expuesto un cliente, en la mayoría de los casos es un daño económico.

Es importante la intervención de un equipo de trabajo o dependencia que promueva lineamientos claros de cómo debe gestionarse un reclamo administrativo, con el personal de *Call Center*, Servicio al Cliente, Plataforma de Servicios u otra dependencia que brinde atención al público, Las dependencias de seguridad son conscientes del proceso y la ayuda que este brinda en una investigación, es crucial que los encargados que reciben al cliente realicen una buena entrevista para saber con certeza las acciones a ejecutar

La unificación de los diferentes sistemas de consulta es necesaria en el proceso de gestión e investigación de eventos maliciosos. Los tiempos de respuesta, a pesar de los esfuerzos que realiza el personal especializado, no son los óptimos, esto conlleva a una serie de situaciones en donde el cliente al final es el más afectado. Y fundamentalmente, la inexistencia de un modelo administrativo que brinde una estructura clara en la detección de fraudes o timos, que no se enfoque en la seguridad que brinda la entidad financiera sino en las vulnerabilidades del cliente. Esto viene a ser la tarea diaria para los departamentos de seguridad y que aún no se logra definir.

4.2.3 Diagnóstico Técnico

Las entidades financieras, incluida Banco Nacional, realizan inversiones considerables en temas de seguridad, esto quiere decir que dentro de sus planes anuales incluyen la actualización de la infraestructura lógica y física de sus dependencias. Cada departamento tiene clara la orientación de sus procesos y conocen las diferentes áreas que requieren o muestran oportunidades de mejora.

Un tema que siempre será cuestionado es la capacidad de cubrir el trabajo diario con el personal disponible, el factor común de los departamentos es si se debe ocupar más recurso humano para poder solventar la demanda, sin embargo, la metodología y la visión de proporcionar una estructura tecnológica robusta, estable y confiable hace que las dependencias estén en constante aprendizaje, atentas a las últimas tecnologías y tratando de aplicar las mejores prácticas.

A pesar de todos los esfuerzos realizados, existen dos puntos clave que son analizados y que en las entrevistas indirectamente se reflejan, primero una comunicación más agresiva en temas de seguridad orientada a los clientes, campañas que se enfoquen en brindar a los usuarios un mayor conocimiento de cómo evitar ser víctimas de fraude y segundo, crear una cultura de responsabilidad, que el cliente adquiera el principio de que los medios de seguridad que posee para ingresar a los productos que la entidad financiera le otorga debe utilizarlos con el mayor cuidado y bajo estrictas normas de confidencialidad.

4.2.4 Entrevistas Diagnóstico de Percepción

Se realizan seis entrevistas, de las cuales cuatro son aplicadas a colaboradores de la plataforma de servicios del Banco Nacional de Costa Rica (ver Anexo 3) y dos a funcionarios de Banca Privada (ver Anexo 4).

Se presentan los resultados a continuación:

Entrevista

Plataforma de Servicios, Oficina Principal.

Banco Nacional de Costa Rica.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A) Explicación breve del objetivo general y de los objetivos específicos.

1. **Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.**

Respuesta #1

Tengo 24 años de laborar para el Banco Nacional, he estado en diferentes oficinas realizando funciones operativas y administrativas, actualmente soy el jefe de la Plataforma de Servicios de la oficina principal.

Dentro de mis funciones básicamente me corresponde velar por que las cosas caminen de la mejor forma posible como un "director de orquesta", que el cliente sea bien atendido en cuanto al tiempo y a la forma, a pesar de que la estructura organizativa de la plataforma no es la misma que algunos años atrás. En resumidas cuentas es un tema de: gestión; seguimiento; de que el control interno se aplique para que el cliente salga satisfecho; de dar seguimiento a casos especiales de clientes o bien de colaboradores. Es una gestión administrativa pero si debo trabajar en temas operativos, estoy a disposición para lo que se necesite.

Respuesta #2

Licenciado en Comercio Internacional, cursando actualmente el bachillerato en contaduría. Mi cargo es el de enlace y análisis de créditos, atender las solicitudes de crédito de los clientes, en cuanto a créditos de consumo, hipotecarios y tarjetas de crédito.

Respuesta #3

Mi experiencia profesional va desde ejercer la contaduría, ya que poseo una licenciatura y estoy incorporada al colegio respectivo, hasta ser cajera, "plantillera" y "plataformista", esto a lo largo de 9 años.

Mi cargo actual es ser plataforma, se atienden todos aquellos clientes que vienen a apertura nuevos servicios, gestiones que otras oficinas no realizan porque no les gusta o no tienen la capacidad o conocimiento competente que deben de brindarles su jefatura o el banco como tal, incentivando talleres o cursos de conocimiento.

Además de que el banco no estandariza los procedimientos a nivel de todas las zonas, si esto existe las jefaturas no logran ponerse de acuerdo para la aplicación de los mismos.

Respuesta #4

Tengo aproximadamente 15 años de laborar en este departamento (Plataforma de Servicios), las funciones son muy numerosas y en algunos casos existen tramites atípicos donde uno mismo debe buscar ayuda con otros compañeros para solventar las diferentes necesidades de los clientes. Sin duda alguna todos los días se aprende algo nuevo.

2. **¿Sabe usted qué es un timo o fraude informático y cómo afectan estos a los clientes?**

Respuesta #1

Sí claro, el timo o fraude informático es buscar la manera de cómo convencer al usuario de que la herramienta suministrada por algún ente financiero es auténtica, y mediante una conversación de confianza, busco que me facilite toda la información que requiero para ingresar yo en sustitución de él.

Si el cliente brinda los datos de sus dispositivos de seguridad para ingresar a los servicios financieros, básicamente está imposibilitando que el banco actúe. El cliente debe ser responsable con sus datos, hacerse de la cultura de responsabilidad digital que le evite entrar en un estado de vulnerabilidad. El problema no son las seguridades, sino la falta de cuidado del usuario al manejar la información para ingresar a los sistemas.

Respuesta #2

En palabras mías, un timo consiste en realizar un acto vandálico a una persona con tal de sacar provecho de ella, la mayor afectación que se presentan en estos casos son la perdida de dineros de las cuentas bancarias o bien tarjetas de crédito en transacciones no realizadas por el cliente.

Respuesta #3

Claro que sí sé qué es un timo o fraude informático, a los clientes los afectan por dos razones, una porque el estafador es muy profesional, y dos porque los clientes son muy confiados, el banco ha invertido cualquier cantidad de dinero en publicidad, mencionado y advirtiendo acerca de los timos que los estafadores utilizan. [Los clientes] No se informan de lo que pasa en la actualidad y brindan información personal y de seguridad cuando se les ha dicho muchas veces que el banco no llama para pedir esa información.

Siempre he mantenido la certeza de que dentro del conglomerado del Banco Nacional algunas personas filtran información de los clientes con cartera potencial, porque el estafador sabe muy bien a quien llamar ya que tiene dinero en su cuenta.

Respuesta #4

Desgraciadamente este tema es el pan de cada día y emocional y económicamente han sido ya muchos clientes afectados por casos de esta índole.

3. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

Respuesta #1

En donde está publicado lo saco por deducción, ya que nunca he llegado a buscarlo, debe estar en la dirección de seguridad establecida cuál es el mecanismo para poder denunciar un fraude vía informática. El tramite es: el cliente se apersona, nos presenta la denuncia respectiva ante el OIJ, se le hace destrucción de la tarjeta, bloqueo de cuentas, se le quita el *token* y se le destruye, se le genera un *token* nuevo, se emite una nueva tarjeta, se procede a levantar las restricciones si el cliente tiene la voluntad de querer levantarlas.

No se puede proceder de oficio porque podría ser que el cliente ya no quiera tener relaciones comerciales con el banco, entonces nos emite una nota y junto con la denuncia se eleva a la gerencia de OP que es la dirección de zona y esta eleva el caso a la dirección de seguridad para que se inicie el análisis respectivo de la gestión, esa es la parte que yo conozco.

Respuesta #2

No, a grandes rasgos sé que se tiene que presentar al banco para presentar su debida queja y posteriormente que haga la investigación. Qué departamento se encarga de esto no sabría.

Respuesta #3

Sinceramente nunca he visto la publicación del procedimiento como tal. Sé que el cliente debe hacer un manuscrito con lo sucedido, traer la denuncia del OIJ, estado de cuenta y cedula, entregarlos en la gerencia para su seguimiento. Cabe mencionar que esto lo sé porque es lo que las jefaturas nos han indicado.

Respuesta #4

El procedimiento como tal sí lo conozco debido a la práctica constante en los diferentes casos, sin embargo, ignoro la ubicación de tal publicación. Importante tomar en consideración que estos procedimientos son constantemente modificados y actualizados.

4. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente?**

Respuesta #1

Debo conocer cuál es la manera efectiva de frenar el fraude desde el punto de vista de las herramientas que utilizamos nosotros, que quiere decir esto: que si un cliente se presenta con una situación lo primero que se debería conocer o hacer es eliminar el dispositivo *token* y si aplica, restringir las cuentas, eso como primeras acciones considerando que somos la cara [del banco] ante el cliente en ese momento. A la vez evitamos entrar en temas de cómo lo estafaron, quién llamó o de dónde solicitaron la información, etc. Considero que el plataformista debe conocer cómo frenar el timo o fraude lo más ágil posible de manera que

no siga causándole un perjuicio económico al cliente, posterior a eso, realizar la investigación que corresponde.

Como recomendación, se debe tratar de concientizar e intentar que el cliente interiorice cuáles son los dispositivos de vulnerabilidad que él tiene al usar una herramienta electrónica, con una sana administración de esos dispositivos se puede garantizar que el cliente no será víctima de fraude o estafa.

Además, se debe informar de manera continua todas las formas en las que los delincuentes pueden timar a las personas por medio de canales electrónicos, esto con el fin de que el cliente este en constante actualización y por ende más prevenido.

Respuesta #2

Conocimiento completo del cliente: a qué se dedica; qué productos mantiene con el banco; cómo son sus movimientos diarios, si se dan; cuáles son los movimientos fuertes en el año. Sobre todo, se debe de mejorar en el tiempo de respuesta por parte del banco.

Respuesta #3

Debe de haber un procedimiento en el mapa de procesos donde yo pueda corroborar cómo realizar la gestión y otra herramienta donde pueda visualizar el seguimiento de la denuncia. Se acercan muchos clientes preguntando al respecto y lo único que podemos hacer el llamar a Noyman para que nos colabore en lo poco que él puede.

Respuesta #4

Los aspectos fundamentales son conocer a fondo cada caso como tal ya que todos tienen diferentes formas o aspectos de haberse efectuado. Una gestión oportuna es bloquear el

Internet *Banking*, reportar y cambiar las diferentes tarjetas de débito o crédito que el cliente posea y adicionalmente cambiar el *token* de seguridad.

Entrevista

Gerencia, Sucursales Digitales.

BAC San José.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A) Explicación breve de Objetivo General y específicos.

1. Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.

Desempeño la función de asistente gerencial en la Gerencia de Canales de Servicios específicamente en el Área de Sucursales Digitales (BAC). Mis función en el departamento es básicamente la administración general operativo-administrativo en el punto de sucursal que me encuentre, manteniendo todos los parámetros de cumplimiento de objetivos, supervisión de personal, seguimiento de proceso.

2. ¿Sabe usted qué es un timo o fraude informático y como afectan estos a los clientes?

Claro, esto es una forma de fraude común en dónde se utiliza diferentes medios tecnológicos para realizarlos. Definitivamente afecta directamente al cliente comprometiendo su información confidencial y exponiéndolo a múltiples circunstancias de fraude (Financiero – Personal).

3. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

No trabajo directamente en esta Área de Fraudes. Sin embargo, mi equipo de trabajo que se relaciona directamente de al cliente; les es común ver este tipo de casos. En el Banco ya tenemos procedimientos establecidos en [los cuales] referimos estos casos por medio de sistemas determinados para que el cliente sea acompañado en el proceso y ejecutar todas las gestiones necesarias para neutralizar el problema, realizar las investigaciones legales y a su vez las devoluciones implicadas.

4. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente?**

Para realizar una gestión oportuna son necesarias las evaluaciones principales del posible fraude:

- Número de cuenta / tarjeta implicada.
- Fechas de realización.
- Comercio afiliado / nombre empresa / página web/ qué giró el cobro.
- Montos globales por fraude.
- Referencia de cobros.

Luego, entendido que un oficial de servicio ingresa la gestión y la recibe un *Backus* del área encargada que la atenderá y ejecutará la resolución correspondiente:

- Tener claro el proceso de la gestión, tanto en etapas como en tiempos de respuesta.

- Es importante comprender los diferentes escenarios comunes de reincidencia de fraudes (actividades normales vs fraudulentas) esto como reconocimiento para poder actuar en ayuda de cara al cliente. No está demás decir que las instituciones financieras deben estar a la vanguardia en los protocolos de seguridad electrónica.

Entrevista

Atención al Cliente, Web Chat.

BAC San José.

Proyecto: **"**Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A) Explicación breve de Objetivo General y específicos.

1. **Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.**

   Funciones generales, atención al cliente por medio de web-chat, atiendo y soluciono las consultas de los clientes por medio de un chat que trabaja 24/7. Nuestro deber es tratar siempre de solucionar al cliente de forma rápida y veraz, ingresar gestiones para que otros departamentos estudien el caso más detalladamente en caso de que así sea necesario o bien ingreso de gestiones para solucionar al cliente su necesidad ya sea para devoluciones, liberaciones, desbloqueos, también guiar al cliente para que se autogestiones por nuestras páginas, etc. En fin, ayudar al cliente con todas sus consultas de una forma clara para que así el cliente cierre de una forma satisfecha.

2. **¿Sabe usted qué es un timo o fraude informático y cómo afectan estos a los clientes?**

En mi opinión, sería el fraude que se realiza de forma electrónica, cuando se roba información del cliente para poder realizar compras, pagos, retiros de dinero con información que se obtuvo por medio de internet o de algún aparato inteligente. Esto afecta gravemente al cliente, ya que se le roba en caso de ser cuentas bancarias, el dinero propio del cliente, en caso de ser información de tarjetas de crédito, hace que el cliente vaya a pagar probablemente por algo que él/ella no solicitó o no obtuvo. Esto podría manchar al cliente ante muchas entidades bancarias o SUGEF, y en casos ya grabes, afectar al cliente haciéndolo pagar grandes cantidades de dinero por algo que no autorizó o bien quedar sin nada de dinero del que tenía ahorrado, por ejemplo.

3. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

Nosotros procedemos con una gestión de estudio legal llamada **contracargo**, esto básicamente se basa en el bloqueo del plástico (y así solicitar uno nuevo con nueva numeración) y haciendo el reclamo por medio de la gestión. Esto se envía a estudio por una cierta cantidad de días, ahora en 24h aproximadamente a muchos de los clientes se le reversa el dinero para que él no se tenga que hacer cargo del mismo, en caso de que el estudio falle a favor , se cierra el caso de forma exitosa, en caso de que no, el dinero se vuelve a debitar.

En este estudio se analizan muchos detalles de la transacción, se conversa con el personal del OIJ, se habla con el comercio, se solicitan cámaras para revisar, entre otras

cosas. Este es el procedimiento al que tenemos conocimiento nosotros como servicio al cliente, no sabría más detalle, ya que de esto se encarga directamente el área de fraudes.

4. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente? Recomendaciones por parte del entrevistado.**

   Es importante conocer el proceso de la gestión para poder explicarla al cliente y que el mismo sienta confianza hacia uno durante este momento tan difícil para él. Tenemos que estar siempre actualizados con la información y con los cambios que se produzcan en las gestiones para el reclamo de fraudes.

   Recomendaciones: no brindar información o fotos de sus cuentas o cédula a terceros; tener cuidado con las paginas por internet que utiliza e ingresa la tarjeta; no responder a correos sospechosos; siempre que haya alguna duda acerca de correos o mensajes que mejor contacte a su banco en primera instancia.

4.2.5 Diagnóstico de Percepción

Se analizaron las entrevistas efectuadas a diversos funcionarios de banca pública y banca privada, para el primero caso Banco Nacional y para el segundo caso BAC San José. El total de los entrevistados realizan labores de atención y servicios al cliente, algunos de una forma más administrativa, siendo el fuerte un tema operativo para ambos.

Los departamentos de atención o servicio al cliente son dependencias que deben conocer los productos y servicios que se les brindan a sus clientes, iniciando por cómo afiliarlos hasta los inconvenientes que a futuro puedan tener, ya sea presencial o mediante la banca digital. La constante actualización sobre estos servicios les da herramientas importantes a los funcionarios

para poder atender a un cliente y brindar un servicio completo acorde a sus necesidades. Como parte de esa actualización, conocer los procedimientos que intervienen en la vinculación de los servicios y su mantenimiento es sumamente importante.

Cuando se conocen los productos o servicios y su relación con el cliente, es más fácil determinar cómo se debe atender un reclamo o una situación de fraude interpuesta por un cliente, cabe mencionar que este desconoce todos los procesos y gestiones, por ende, llama o se apersona a la entidad bancaria para que solventen su problema. Es ahí en donde la existencia de lineamientos fuertemente establecidos y publicados para el conocimiento de todos los funcionarios, son vitales en la correcta gestión de este tipo de incidentes. Sin embargo, como se pudo determinar en las entrevistas, el criterio sobre la existencia del procedimiento para la atención de reclamos administrativos enfocados a timos o fraudes informáticos es mínimo e inconstante.

El cliente debe ser una prioridad para cualquier entidad que brinde servicios, por ende, uno de los principales pilares es salvaguardar sus intereses y aún más si estos son económicos. Un cliente satisfecho no solamente se ve cuando se le brinda un asesoramiento completo, sino también cuando presenta alguna situación que le afecte directa o indirectamente y esta situación es resuelta de forma eficiente, amplia y clara.

4.3 DETERMINACIÓN DE BRECHAS

Para realizar el análisis de brechas, se elaboró un diagnostico FODA el cual contempla: la situación actual; deficiencias y aspectos de mejora que requieren las dependencias involucradas en la atención del cliente; gestión de reclamos administrativos y las direcciones encargadas de la seguridad informática y de la seguridad de la información; todas enfocadas en la detección y prevención de fraudes en su sistema financiero.

Tabla 4*: FODA Determinación de Brechas*

F	O	D	A
Departamentos debidamente estructurados y definidos para la gestión de seguridad informática.	Optimizar los procesos con base en las mejores prácticas internacionales en temas de seguridad.	Esfuerzos aislados de la organización en temas de seguridad.	Ingeniería social.
Inversión constante en actualización de equipo lógico y físico.	Inclusión de nuevos sistemas de control y protección enfocados a CRM.	Ausencia de una comunicación asertiva entre los departamentos de cara al público y los departamentos técnicos.	Carencia de cultura y responsabilidad en la utilización de servicios electrónicos.
Personal especializado para la atención de incidentes.	Modelos basados en Inteligencia Artificial que establezcan las reglas de negocio en temas de detección y prevención de fraudes informáticos.	Toma de decisiones condicionadas que ralentizan los procesos.	Digitalización Bancaria.
Sistemas de información, políticas, lineamientos y procedimientos establecidos.	Unificación del sector financiero en propuestas de seguridad informática; estrategias aplicadas a sus sistemas o servicios electrónicos.	Diversidad de sistemas de información.	Disponibilidad de recurso económico.
		Tiempo de respuesta a incidentes.	Vulnerabilidades de los usuarios.

Fuente: Elaboración Propia

CAPÍTULO V:

DISEÑO Y DESARROLLO DEL PROYECTO

5.1 DESARROLLO DE LA PROPUESTA DE TRABAJO.

Basado en la metodología planteada en el capítulo III, en donde se toma como referencia la Tabla 3: Matriz de Coherencia, se plantea el desarrollo de la propuesta de solución para el proyecto. La distribución de las fases identificadas especialmente para este proyecto responde a la necesidad de cada objetivo, los cuales tienen los aspectos a considerar para cumplir con el objetivo general.

Si bien es cierto en la Tabla 3: Matriz de Coherencia, se mencionan cuatro fases, sin embargo, para el desarrollo de la solución se proponen cinco fases las cuales contendrán la propuesta o rúbrica a seguir para el desarrollo del modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario.

5.1.1 Fase Uno: Identificación de Vulnerabilidades.

El objetivo principal de esta fase es identificar las vulnerabilidades más críticas a las cuales está expuesto un cliente al utilizar los servicios en línea o presenciales. Es importante mencionar que, cuando un cliente se vincula a una entidad financiera mediante un contrato de servicios bancarios, por ejemplo, automáticamente es candidato para utilizar todo el catálogo de servicios que la entidad ofrece.

La entidad financiera debe ofrecerle al cliente la plataforma tecnológica correspondiente para que realice sus operaciones o transacciones acorde a su actividad comercial. El cliente deberá proporcionar la documentación e información pertinente para que la entidad financiera pueda brindar la mejor asesoría teniendo un mayor conocimiento de su perfil, todo esto amparado en las leyes y políticas financieras gubernamentales e internacionales.

El departamento encargado de la administración del modelo de perfil y comportamiento transaccional en conjunto con los departamentos de gestión comercial, deberán analizar lo siguiente:

- Información actualizada del cliente.
- Productos y servicios financieros que posee el cliente.
- Frecuencia de uso de los productos y servicios financieros.
- Servicios digitales de mayor vinculación.
- Dispositivos de seguridad que utiliza el cliente ligados a esos servicios.

En base con los aspectos anteriores y a los principios relacionados a la inteligencia artificial, tomando como referencia la lógica de las redes de contra propagación, se tendría el primer insumo que necesita el modelo de perfil y comportamiento transaccional. Este se resume en una serie de entradas que serán evaluadas posteriormente contra la información que ya mantiene la entidad financiera acerca del cliente.

Según las experiencias identificadas en la plataforma de servicios, los clientes experimentan las siguientes vulnerabilidades de cara a los servicios presenciales y electrónicos que ofrece la entidad:

- Resistencia al cambio tecnológico y a la banca digital.
- Desconocimiento de procesos y trámites automatizados o actualizados por la entidad financiera.

- Desconocimiento de normativas y políticas bancarias.

- Mal uso de los dispositivos electrónicos de seguridad, como *token*, claves dinámicas, contraseñas, firma electrónica, mensajes de verificación, etc.

- Falta de capacitación del personal en la colocación de servicios.

- Ingeniería social por parte de grupos delictivos.

- Tiempos de respuesta por parte de los departamentos de seguridad en la solución de incidentes o eventos maliciosos

Las entidades financieras en sus diferentes sistemas y bases de datos poseen toda la información vital de un usuario, por ejemplo, datos personales, perfil financiero, récord crediticio, representaciones jurídicas, etc. Teniendo conocimiento de estos datos, el modelo en su primera fase tendrá como resultado valorar las vulnerabilidades externas e internas que posee un cliente, además de las transacciones que generalmente el usuario realiza y por cuáles canales las ejecuta. Al ser un modelo de inteligencia artificial la fase de identificación de vulnerabilidades será sumamente importante en la fase dos y tres.

5.1.2 Fase Dos: Justificación de Modelos Internos y Externos

Para el desarrollo de esta fase, es importante que los departamentos encargados de la seguridad informática, seguridad financiera o bancaria y seguridad de la información en términos generales asignen a cierto número de colaboradores la función de evaluación de procedimientos, políticas, modelos entre otras guías referentes a la gestión, detección y prevención de fraudes informáticos.

Las entidades financieras poseen procedimientos y lineamientos que habitualmente no se actualizan, más cuando esos procesos solucionan de manera muy global un evento o una situación específica. Si este tipo de eventos no ocasionan un daño económico directo y sustancial, con mucha más razón el proceso podría mantenerse por periodos considerables de tiempo sin ser renovado. La fase de evaluación de modelos internos y externos pretende eliminar esa práctica.

El equipo de trabajo al cual se le asigne esta fase deberá mantener un ideal de investigación, innovación y desarrollo buscando siempre optimizar recursos y procesos en el mejoramiento de estrategias tecnológicas que fortalezcan la estructura lógica y física de sus dependencias y áreas asociadas.

Como punto de partida hacia la evaluación de modelos, el equipo de trabajo podrá utilizar preguntas que delimiten su análisis, por ejemplo: ¿Qué estamos haciendo? ¿Cómo lo estamos haciendo? ¿Qué tipo de modelos de referencia puedo encontrar en el mercado? ¿Qué características tienen? ¿Cómo puedo aplicarlos en mis procedimientos o modelos internos? ¿Qué dicen las compañías internacionales que brindan servicios de ciberseguridad? ¿Qué proponen las entidades estatales en temas de seguridad informática?

Al equipo de trabajo, posterior a la realización de esta investigación, la cual deberá de hacerse periódicamente, le corresponderá presentar un informe detallado de los resultados obtenidos. Este informe debe contener primordialmente todos aquellos hallazgos tecnológicos que tengan como fin brindar las mejores prácticas en cuanto a temas de seguridad informática orientados a la detección y prevención de fraudes. Es fundamental que se identifiquen procesos, lineamientos, estratégicas que en ese momento no se estén implementando en la entidad financiera, de manera que los departamentos especializados los reestructuren y apliquen a sus dependencias.

La propuesta en esta fase es utilizar una ideología de "*benchmarking"*, que permita realizar estudios periódicos y comparaciones a nivel del sistema financiero nacional e internacional con el fin de aplicar las mejoras correspondientes y fortalecer las primeras etapas del modelo de perfil y comportamiento transaccional.

5.1.3 Fase Tres: Valoración Del Perfil y Comportamiento del Cliente

El desarrollo de esta fase tiene como insumo principal las vulnerabilidades encontradas en la fase uno y el informe presentado en la fase dos, el cual brindará una serie de recomendaciones aplicables a los procesos actuales. Sin duda, es importante conocer las necesidades del cliente y posibles situaciones de riesgo en donde se pueda ver expuesto, enfocándose en un criterio externo. Cuando se identifican las vulnerabilidades, el siguiente paso es analizar los productos o servicios que el cliente posee en la entidad y como estos se podrían ver afectados.

Como se indica en el capítulo dos del presente documento, un perfil es una serie de rasgos que caracterizan algo; para este caso serian rasgos que caracterizan a un cliente, entonces se debe analizar qué tipo de cliente tenemos. Para tal efecto, considerar lo siguiente:

- **Información o datos personales:**

  Se refiere a todos la información que permita conocer datos generales del cliente, por mencionar algunos: estado civil, direcciones domicilio o trabajo, correo electrónico, números telefónicos, profesión u ocupación, lugar de trabajo, etc.

- **Principal actividad económica:**

  Es importante conocer a que se dedica el cliente, puede presentar varias actividades económicas como públicas, privadas o semiprivadas, pero dependerá de la principal con el

fin de saber qué productos o servicios financieros son aplicables, teniendo como resultado una minimización del riesgo.

- **Fuentes de ingresos:**

  Con el fin de tener amplio conocimiento de la procedencia de los fondos, amparado en la ley gubernamental 8204 sobre legitimación de capitales, conocer las fuentes de ingreso del cliente garantizará la legalidad de su operativa bancaria.

- **Relaciones financieras con terceros:**

  Cuando un cliente mantiene relaciones financieras con terceros, ya sea por administración de fondos, representaciones legales o servicios y productos vinculados con otra entidad, es importante determinar que tan comprometido puedo estar, ya que existen entes reguladores que mantienen ciertos parámetros los cuales deben ser seguidos por las entidades financieras.

  Cabe mencionar que el análisis de la información es un trabajo conjunto con las dependencias interesadas en desarrollar el modelo, por ende, la existencia de una comunicación entre los departamentos es la clave para que las fases se logren con éxito. Dependerá de la administración crear esos puentes de comunicación y coordinar lo necesario para que la información sea los más completa, exacta y oportuna.

  Por otra parte, se debe analizar el comportamiento transaccional del cliente, esto quiere decir que una vez analizado el perfil, todo cliente tiene un comportamiento posterior a su vinculación con la entidad financiera. Este comportamiento se basa en la actividad que tiene el cliente con los servicios electrónicos o presenciales. Para poder determinar cuál es ese comportamiento se debe conocer qué tipo de productos utilizada el cliente y con qué frecuencia los utiliza.

Dentro de ese comportamiento es significativo considerar que pueden existir transacciones o movimientos financieros que no correspondan al flujo normal de las transacciones realizadas por el cliente, sin embargo, es ahí en donde el modelo mediante inteligencia artificial, solución que se desarrollara en la fase cuatro, debe discriminar mediante factores ligados al perfil del cliente si esa transacción es correcta, aplicable y propia.

5.1.4 Fase Cuatro: Solución Estratégica de Inteligencia Artificial.

En fases anteriores se ha venido trabajando y analizando los diferentes factores determinantes para entender la propuesta del modelo de perfil y comportamiento transaccional. Identificar las vulnerabilidades de los clientes, conocer el entorno financiero mediante modelos internos y externos enfocados a la prevención de fraudes informáticos y el análisis del perfil y comportamiento del cliente. Estos puntos se convierten en la principal estructura para plantear una guía de solución estratégica basada en inteligencia artificial.

Para la propuesta de solución es fundamental que la entidad financiera cuente con un presupuesto o solvencia económica para la inversión de la plataforma tecnológica correspondiente, si ya la posee, de igual forma será importante que analice la actualización de ciertos aplicativos con el fin de que el modelo se aplique de la mejor manera. Al ser un modelo basado en inteligencia artificial la infraestructura tecnológica tanto física como lógica debe estar acorde a las últimas tendencias orientadas al aprendizaje de máquina, la inteligencia de negocio y al análisis de datos en gran volumen. Además debe existir compatibilidad con las herramientas o aplicativos que existen en el mercado. Bajo esta línea dependerá de la entidad buscar los socios de negocio que brinden respaldo en todo el proceso de implementación del modelo o bien capacitar al personal interno según sus necesidades.

La estrategia planteada se divide en cuatro etapas, independientes a las fases desarrolladas para la solución del proyecto. Cada etapa contendrá un proceso de inteligencia artificial basado en los conceptos mencionados en el capítulo dos del presente documento, además cumplir con la metodología mencionada en el capítulo cuatro.

A continuación, las etapas mencionadas:

- **Etapa 1: Llave y Segmentación:**

  En la etapa uno se tendrán dos factores importantes, el primero es el cliente, el cual tendrá una posición de llave. La función de llave permite enfocar el análisis al comportamiento único del cliente, su identificación será el método de consulta para los productos o servicios electrónicos que utiliza.

  El segundo factor será la segmentación del cliente. Cada usuario de una entidad financiera, según su perfil y comportamiento, es asociado a un segmento; estos segmentos podrían darle ciertos beneficios financieros y confiabilidad por parte de la entidad, ya que se conocen sus operaciones. Esta etapa pretende clasificar a los usuarios y clientes para la etapa dos.

- **Etapa 2: Orientación y Enfoque:**

  Es importante considerar la orientación y el enfoque del modelo, razón por la cual, en esta etapa, el equipo de trabajo deberá definir limites en los análisis a realizar. Como se ha venido desarrollando en el proyecto, la orientación y el enfoque será aplicado a todas aquellas transacciones, operaciones o movimientos financieros que muestren rasgos inusuales en el comportamiento de un cliente, además se considerarán con un mayor nivel de interés transacciones mediante canales o servicios electrónicos, siendo estos los más vulnerables puesto que generan mayor impacto a los clientes.

- **Etapa 3: Rating e Historial de Madurez:**

Para esta etapa se van a definir dos factores, los cuales deberán ser caracterizados acorde a las políticas financieras de cada entidad, además ya se deberá contar con una plataforma de análisis de datos o sistema informático que implemente Machine Learning.

El primer factor será la creación de un *rating* de clientes, el cual pretende calificar a los usuarios acorde a su comportamiento en la entidad financiera. A manera de ejemplo, cuando un vendedor promociona artículos en una tienda online y obtiene calificaciones positivas posterior a sus ventas por parte de los compradores, este vendedor se vuelve confiable y seguro; es lo que se espera de este *rating* de clientes, que la administración y los departamentos encargados de la seguridad informática minimicen los controles cuando un cliente tiene un *rating* alto y así poder utilizar esos recursos en otro tipo de operaciones.

Ligado al rating de clientes, está la creación del historial de madurez el cual deberá utilizar la lógica de *Deep Learning*. Este factor pretenderá generar un análisis del entorno del cliente, por tal razón el estudio de los datos debe ser abarcado desde las diferentes herramientas de información que posea la entidad financiera, de manera que todos los datos que se conozcan acerca del usuario puedan ser evaluados y analizados con el fin de determinar la relación con terceros (aclarar que esta relación con terceros se enfoca a una vinculación bancaria entre usuarios).

El resultado de este historial de madurez brindará información importante sobre el cliente y sus movimientos, que mediante procesos de *Big Data* serán presentados y configurados en los sistemas internos de la institución, con el fin de brindar una mayor trazabilidad. También, mediante la lógica que brinda las redes de contra propagación, este historial estará en constante cambio, evaluando comportamientos financieros.

El objetivo principal de esta etapa consiste en que la entidad financiera teniendo conocimiento del perfil del cliente, el rating generado por su actividad económica y el historial de madurez acorde a su comportamiento transaccional pueda determinar bajo criterios ya activos de inteligencia artificial y aprendizaje de máquina, los controles que deberán ser aplicados a mayor o menor escala. Además, la entidad financiera podrá reclasificar su condición con el fin de ubicarlo en una posición diferenciada a los demás clientes, pero teniendo claro que estará en constante evaluación, de manera que cualquier cambio detectado alterará automáticamente su segmento y su clasificación.

- **Etapa 4: Presentación de Datos**

  Esta etapa lo que pretende es la creación de un entregable, el cual permita a la administración tomar las decisiones correspondientes de tal manera que oriente al negocio con la aplicación de medidas a nivel comercial y de seguridad informática.

  El informe o entregable deberá contener resultados detallados de las etapas anteriores, considerando que para esta sección se cuenta con el material necesario y sustentable que concluye con el propósito del modelo de perfil y comportamiento transaccional. La información presentada debe mostrar como estructura básica de análisis post modelo:

  - Datos personales del cliente.
  - Inicio de relación comercial con la entidad.
  - Servicios o productos vinculados.
  - Situación financiera de los últimos meses (periodos definidos por la entidad financiera).

- Situación financiera actual.
- Comportamientos transaccionales.
- Proyecciones clasificatorias según comportamiento.
- Segmentación y Calificación.
- Parámetros generales del negocio.

En el mercado existen herramientas que permiten almacenar temporalmente y mostrar este tipo de información, por mencionar algunas como referencia, tecnologías como DataLakes, Tableu, OBI, Power BI, Cloudera, etc.; dependerá de cada entidad realizar los acuerdos comerciales con proveedores tecnológicos que brinden o refuercen sus plataformas para la ejecución del modelo.

En el capítulo seis del presente documento se brindarán algunas recomendaciones sobre el uso de estas tecnologías.

5.1.5 Fase 5: Guía de Mejora Continua

Todo modelo estratégico orientado a la solución de un problema o necesidad, el cual debe contemplar dentro de su estructura un proceso de actualización y mejora continua, de manera que cada área que es desarrollada se adapte a cambios circunstanciales.

Este proceso puede ser implementado de diferentes formas, sin embargo, para efectos del modelo de perfil y comportamiento transaccional en la detección de fraudes, debe ser planteado mediante los principios de inteligencia artificial, razón por la cual la entidad financiera, para esta fase, también deberá contar con una plataforma tecnología que le permita auto administrar la revisión periódica de cada área del modelo. Se debe considerar como principal tecnología a utilizar

los fundamentos de las redes de contra propagación, cumpliendo la teoría de un aprendizaje mediante experiencias.

La construcción y gestión del cronograma de mejora continua pretende, mediante indicadores establecidos por el equipo de trabajo especializado, hacer evaluaciones constantes con el fin de reforzar cada fase mencionada en el presente capítulo, acorde a las mejores prácticas nacionales e internacionales.

Para tal efecto se sugiere a continuación una serie de indicadores que podrán ser valorados por el equipo de trabajo encargado de monitorear el modelo:

- Eventos o situaciones presentadas durante el mes.
- Capacidad de respuesta y solución.
- Rendimiento de ejecución de las fases del modelo.
- Afectación económica por cliente, por zona comercial y cartera general de clientes.
- Cambios en normativa, políticas o procedimientos internos o externos.
- Cumplimiento de objetivos estratégicos.
- Rentabilidad del modelo en general.

Corresponderá a la administración y asesoría del equipo de trabajo definir mediante políticas internas los periodos de evaluación y la frecuencia. En el capitulo seis del presente documento se mencionarán algunas recomendaciones con respecto a estos tiempos.

Como entregable se deberá emitir un informe del estatus del modelo abarcando todas las fases, brindando aspectos clave de mejora y observaciones puntuales, de manera que la administración tome las decisiones necesarias y coordine con las dependencias involucradas lo que considere pertinente.

CAPÍTULO VI:

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

En relación con el desarrollo y la propuesta de solución planteada en este documento, se formulan las siguientes conclusiones fundamentadas en los objetivos de la investigación.

- El modelo de perfil y comportamiento transaccional en la detección de fraudes establece una guía aplicable para cualquier entidad financiera que brinde servicios al público. Según lo antes mencionado, la entidad financiera Banco Nacional, no solo fue fuente importante de información sino candidata para la aplicación del modelo.

- Se concluye que la utilización de las entrevistas y la observación de los procesos, fueron herramientas fundamentales para determinar las brechas operativas para la guía de solución.

- Se determina que, para obtener resultados positivos al implementar el modelo, debe existir un compromiso conjunto entre las dependencias interesadas de la entidad financiera, la creación de procedimientos y el enfoque de estos deben ser congruentes e integrales a la propuesta planteada.

- No se define una tecnología única de aplicación, cada entidad deberá ajustar su plan estratégico y presupuesto acorde a sus necesidades.

- Se carece de un ente administrativo centralizado que delimite responsabilidades y estandarice la toma de decisiones en el cumplimiento de los objetivos del proyecto.

- Se concluye que la comparación de diferentes modelos, tecnologías, normas y buenas prácticas permitieron contraponer lo utilizado por la institución de referencia, con lo utilizado en el mercado actual.

- El costo de implementar un modelo de perfil y comportamiento transaccional es sumamente bajo en relación con las pérdidas principalmente económicas que puede tener una entidad financiera cuando sus clientes son víctimas de fraude.

- Se determina que el uso de la inteligencia artificial en los procesos financieros debe ser analizado según las políticas internas institucionales, por ende, los insumos para el aprendizaje automático del modelo deberán ser suministrados por las áreas comerciales y de atención al cliente.

6.2 RECOMENDACIONES

A continuación, se brindan algunas recomendaciones sobre aspectos importantes en el desarrollo e implementación del modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario.

- Se recomienda que el modelo de perfil y comportamiento transaccional sea incluido en los planes estratégicos institucionales de tecnologías de información, teniendo conocimientos generales e iniciativas claras en temas de inteligencia artificial, orientados a los servicios de TI que brindan.

- Es fundamental que los colaboradores involucrados en el modelo realicen un proceso de capacitación, de manea que se minimice la curva de aprendizaje y gestión de cambio de los procesos.

- Es importante que las herramientas tecnológicas estén sometidas a una mejora continua por parte del ente encargado, permitiendo que el proceso esté en constante actualización y satisfaga las expectativas de la organización.

- Las herramientas disponibles en el mercado que trabajan con principios de inteligencia artificial mencionadas en el capítulo cinco, fase cuatro, en lo referente a la presentación de datos, deben ser orientadas a los resultados que desee obtener la organización, evaluando su viabilidad y factibilidad.

- Con respecto a los periodos de evaluación y frecuencia del cronograma de mejora continua, se recomienda para el primer año periodos trimestrales, para el segundo año y posteriores, periodos semestrales.

- Determinar una segregación de responsabilidades y funciones entre las dependencias interesadas, además de establecer niveles de autorización requeridos durante la realización de cada proceso de implementación.

- Es importante que se documente de forma digital todos los procesos y cambios relacionados a la implementación del modelo, con el fin de tener los respaldos necesarios o restauración de etapa.

APÉNDICES Y ANEXOS

7.1 ENCUESTAS

Anexo 1 Entrevistas, Dirección de Seguridad

Entrevista

Banco Nacional de Costa Rica.

Dirección de Seguridad.

Sr. Martin Alvarado Vargas.

Proyecto: “Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario”

A. **Explicación breve de objetivo general y específicos**.

1. **Don Martin, para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.**

   Tiene amplia experiencia en temas de seguridad, cuento con más de 20 años laborando para el Banco nacional. Anteriormente trabajé para el Organismo de Investigación Judicial (OIJ) como investigador y oficial de campo. Actualmente desempeño el cargo de jefe de seguridad en la Dirección de Seguridad del Banco Nacional y como jefe de seguridad velo por todos los aspectos administrativos relacionados a las diferentes situaciones que se presenten en las oficinas en temas de fraudes, estafas, asaltos, entre otros eventos delictivos.

2. **¿Cómo se realiza actualmente el proceso de gestión del fraude materializado (servicios digitales)?**

Según Alvarado, el cliente primero debe interponer un reclamo administrativo en cualquiera de los siguientes canales: Centro de llamadas, Contraloría de Servicios o en la red de oficinas del Banco Nacional. Posteriormente, el cliente debe presentar una denuncia formal ante el OIJ, seguidamente llevar toda la documentación a una oficina del Banco para que sea recibida por el personal correspondiente.

La información será analizada con el fin de determinar la veracidad del fraude y proceder a realizar las acciones según los procedimientos establecidos por la institución y las leyes judiciales del país.

3. ¿Cuáles son las dificultades en ese proceso actualmente?

Básicamente, las principales dificultades de este proceso se resumen en la revisión de la información en las distintas bases de datos. La información que se requiere para la investigación no está recopilada en una sola herramienta, lo que ocasiona atrasos en la creación de reportes.

Por otra parte, el recurso humano a pesar de que cuenta con herramientas individuales no es el suficiente para hacerle frente a la cantidad de casos que se reciben en el departamento, presentándose nuevamente la misma problemática en los tiempos de espera.

Diagnostico Operativo

4. ¿Qué procedimientos, políticas o reglamentos internos se aplican a cada etapa?

Bueno, se aplican todos los procedimientos y políticas establecidas en mapa de procesos, sección que se encuentra en la Intranet del Banco Nacional. Estos procedimientos brindan

instrucciones técnicas para la gestión y atención de los diferentes eventos que correspondan a la Dirección de Seguridad.

5. **¿Se aplican correcta y linealmente los procedimientos, políticas o reglamentos internos?**

   Es importante considerar que todos los casos que nosotros recibimos en el departamento por más simples que sean deben llevar un orden y un avance en cada etapa que sea congruente con los procedimientos establecidos por la institución. No podemos omitir detalles debido a que estos casos pueden ser solicitados por dependencias judiciales o auditorías externas e internas.

6. **¿Cómo debería ser la operativa según su opinión y experiencia en el proceso?**

   Debería ser más expedita, que podamos procesar la información con mayor facilidad, simplificando trámites y tiempos de espera. Acceso a sistemas de información los cuales hoy en día son administrados en otros departamentos y para solicitar información debemos interponer un requerimiento, evidentemente esto genera tiempos y atrasos en el proceso.

Diagnostico Técnico:

7. **¿Con cuáles herramientas (infraestructura física o lógica, sistemas, aplicaciones) cuenta el departamento de seguridad para el registro de los fraudes?**

   Desde el punto de vista de sistemas contamos con herramientas como: el SFB, el cual es un sistema de consulta de movimientos y transacciones de las cuentas de los clientes; el Portal Integrado de Servicios, el cual contiene diversa información de los clientes como por ejemplo datos personales, perfil financiero, productos o servicios asociados, entre

otros; bases de datos transacciones, las cuales son administradas por el departamento de seguridad informática del banco; y otra base de datos pero enfoca un poco más a la información policial administrada directamente por nosotros el equipo de la Dirección de Seguridad.

En cuanto a infraestructura física, contamos en todas las oficinas del país con un circuito cerrado de cámaras, las cuales poseen las características necesarias para identificar cualquier situación que se presente. Brindamos charlas a diferentes departamentos con el fin de capacitar el personal (ejecutivos de cuenta, plataforma de servicios, servicio al cliente, etc.) en temas de seguridad y que sean ellos mismos los que trasmitan recomendaciones a sus clientes en el uso correcto de sus cuentas, además de la información que el Banco se encarga de comunicar en los diferentes medios o redes sociales.

8. **¿Considera que el equipo actual (colaboradores y recurso tecnológico) cumplen con los objetivos y alcances del departamento?**

En el departamento de seguridad contamos con un recurso humano conformado por profesionales en áreas como administración e ingeniería, sin embargo, para efecto de sus funciones han ampliado sus conocimientos en temas de seguridad e investigación, lo que se quiere decir es que han aprendido a desarrollar sus funciones, aunque sus profesiones no se relacionen, es un tema de aprendizaje constante y experiencia día a día.

Se cumple con los objetivos a pesar de las limitantes, pero no por el personal, sino por las herramientas que se utilizan para el desarrollo de las investigaciones, que es lo que comentábamos anteriormente. Sería de gran ayuda tener un sistema o una plataforma que

nos facilite la operativa, y por qué no un modelo que reúna ciertos criterios de las demás herramientas y que simplifique las gestiones que realizamos.

9. **¿Qué mejoras sugeriría usted para ambas áreas?**

Definitivamente mayor recurso humano para hacerle frente de forma más rápida a los eventos que se reciben en el departamento. Como lo hemos venido conversando, una plataforma en donde podamos encontrar unificada toda la información que necesitamos o bien un modelo que simplifique la operativa.

CONSENTIMIENTO

Fecha: 22 - 11 - 2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Entrevista

Banco Nacional de Costa Rica.

Dirección de Seguridad.

Sr. Noyman Brenes Aguilar.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. **Explicación breve de objetivo general y específicos**.

1. **Don Noyman, para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.**

   Tengo 16 años de experiencia a nivel de seguridad bancaria, soy graduado en criminalística. Las funciones que realizo acá en la Dirección de Seguridad tratan de temas de asistencia a la parte investigativa sobre cualquier tipo de fraude que se pueda llevar acabo o donde exista una noticia de crimines expuesta por parte de algún cliente, es ahí donde nosotros llegamos a actuar. Dentro de los tipos de fraude que se logran establecer serian fraudes con cheques, timos de depósito, ventas por internet con el fin de obtener información sensible para conocer datos del cliente y posteriormente realizar una estafa y lo que está más en boga, son los fraudes mediante servicios electrónicos o fraudes informáticos.

2. **¿Cómo se realiza el proceso de gestión del fraude materializado (servicios digitales)?**

   Se puede hacer de dos formas, que el cliente llame y avise a nuestro centro de contacto o que se apersone a una oficina bancaria, también puede suceder que el afectado no realice el reclamo en el banco, más sin embargo lo realiza ante el OIJ. Cuando el cliente realiza la

gestión mediante el centro de contacto, el personal se encarga de deshabilitar todos aquellos servicios que estén ligados electrónicamente a los principales productos del cliente los cuales puedan poner en peligro su capital; finalizado este proceso el cliente deberá apersonarse a una agencia del Banco a continuar con el proceso administrativo correspondiente. Si el cliente se presenta al Banco directamente, será el plataformista quien se encargue de realizar la gestión y remitirnos el caso a nosotros una vez concluida la etapa de desafiliación de servicios.

Si el cliente realiza el reclamo ante el OIJ, será este organismo quien notifique al banco que un cliente el cual mantiene relación comercial con la institución presenta un posible fraude y con base a esa información nuestro departamento se encargará de realizar el debido proceso; es importante mencionar que para las gestiones anteriores siempre se debe identificar el tipo de fraude para poder canalizar la investigación de la mejor forma posible.

3. **¿Cuáles son las debilidades en ese proceso actualmente?**

Muchas veces sucede que no hay un pronto alcance a la información, ya que el cliente cuando llama o llega al banco no es muy claro con lo que está solicitando, entonces el personal del Banco debe extenderse en entrevistar para definir realmente cual es la situación del cliente y proceder con los bloqueos correspondientes. Para el banco es sumamente importante la primera información, es vital para poder actuar con el fin de detener o prevenir un daño mayor al cliente.

Diagnostico Operativo:

4. **¿Qué procedimientos, políticas o reglamentos internos se aplican?**

Para los funcionarios existe una matriz establecida para el protocolo de atención en caso de fraudes, ya sea por canales electrónicos, transferencias, etc., ya está parametrizado lo que tiene que hacer, cuáles son el a, b, c de lo que tiene que hacer. Esta información se ubica en la intranet, en el mapa de proceso, completamente público para el funcionario y a las jefaturas para que lo tengan presente en sus oficinas ante cualquier situación.

Ahora bien, si existiera alguna situación atípica, sin ningún problema pueden llamar a nuestra dirección y con gusto podemos guiarlos o asesorarlos de la mejor forma posible para que puedan atender y gestionar la necesidad del cliente, máxime que algunos de ellos no tienen un solo servicio o una sola cuenta, sino que tienen diferentes productos con la institución y es importante determinar cuáles han sido afectados y cuáles deben bloquearse temporalmente.

5. **¿Se aplica correcta y linealmente los procedimientos, políticas o reglamentos internos?**

Sí se aplican, pero siento que no a cabalidad tal vez porque falta un poco de *expertise* por parte del funcionario sumado a que el cliente, como lo mencioné anteriormente, no es muy claro, entonces se entra en un proceso de adivinar incluso la gestión que requiere el cliente. Para disminuir estas discrepancias, lo primero que se tiene que realizar y lo que nosotros le indicamos primero al funcionario es sacar al cliente de Internet Banking y BN Móvil, con el fin de cerrar portillos lo antes posible

6. **¿Cómo debería ser la operativa según su opinión y experiencia en el proceso?**

Deben existir cambios, el Banco Nacional no se puede quedar en una sola matriz o proceso, ya que el fraude va llegar a mutar y a ofender, entonces deben haber constantes modificaciones en este caso de cada una de las áreas expertas o involucradas de crear los sistemas o procesos de seguridad, de manera que estén en continua actualización, porque el fraude siempre será fraude pero la modalidad que se utiliza es la que será diferente, por ende, debemos estar enfocados en atacar esas modalidades y tratar de reducir con medios informativos la vulnerabilidad que en la que se encuentran los clientes.

Diagnostico Técnico:

7. **¿Con cuáles herramientas (infraestructura física o lógica, sistemas, aplicaciones) cuenta el departamento de seguridad para el registro de los fraudes?**

Partimos de que sabemos cómo operan los delincuentes, cómo llegan al cliente, la forma en la que aplican una ingeniería social a una población con mayor vulnerabilidad, cómo se aprovechan de situaciones sensibles para materializar el timo o fraude conociendo que carecen de esa malicia.

Desde el punto de vista de nuestro departamento, tenemos herramientas de revisión, de verificación, de análisis que provee el banco como lo son: el SFB; archivo virtual; el sistema de tarjetas de visa; bases de datos de IB, las cuales son importantísimas; el sistema de video electrónico, el cual nos sirve como evidencia ante un proceso solicitado por el OIJ; tenemos también bases de datos de reconocimiento de personas, de manera que se puede hacer una identificación primaria para que posteriormente el OIJ realice la investigación de campo según corresponda.

8. ¿Considera que el equipo actual (colaboradores y recurso tecnológico) cumplen con los objetivos y alcances del departamento? ¿Qué mejoras consideraría?

Definitivamente considero que somos pocos, en relación con la gran cantidad de casos que ingresan por los diferentes canales de recolección de incidentes; el uso tecnológico es un factor, es fuerte, pero se necesitan más herramientas a la mano. Debemos acudir a varios departamentos para solicitar la información, esto evidentemente genera atrasos en los tiempos de respuesta.

La ausencia de un módulo que reúna todas las herramientas en un solo acceso en donde podamos obtener los insumos que requerimos para las investigaciones, sería de las mejoras que sugeriría, esto con el fin de no depender de otros departamentos y solventar los casos a la mayor brevedad posible.

El cliente tiene una gran responsabilidad y peca al no tomar esa responsabilidad como debe ser, no informarse, no entender de manera clara la información que se le brinda o hacer caso omiso a esa información, básicamente se define como una ausencia de cultura en términos de seguridad y el banco, como ente proveedor de servicios, debe esforzarse por ser más agresivo, si se puede llamar de esa manera, en comunicarle a los clientes las consecuencias que se pueden tener en suministrar a un tercero datos sensibles relacionados a productos financieros. Al final es un trabajo en conjunto de ambas partes para que el cliente haga conciencia de la forma en que utiliza los servicios y que el banco le brinde actualizadamente mecanismos confiables e información oportuna; aplicando esto no solo para Banco Nacional sino para todas las entidades financieras.

CONSENTIMIENTO

Fecha: 6-12-2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Entrevista

Banco Nacional de Costa Rica

Dirección de Seguridad

Sr. Joaquín Arias Robles

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. Explicación breve de objetivo general y específicos.

1. Don Joaquín, para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.

Tengo más de 14 años de experiencia en temas de seguridad en el Banco Nacional [desde que] el tema de los fraudes no se conocía o era muy nuevo en entidades financieras. De profesión, soy licenciado en ingeniería en sistemas y desde junio del 2017 estoy realizando mis funciones en la Dirección de Seguridad y soy el único experto en análisis de reclamos administrativos mediante internet *banking.*

2. ¿Cómo se realiza el proceso de gestión del fraude materializado (servicios digitales)?

Desde el 2005 el Banco Nacional ha venido gestionando todas las modalidades de eventos delictivos en torno a sus servicios electrónicos, algunas de las cuales han sido simples pero funcionales para su época, en otras palabras, han logrado su cometido. En el 2008 implementamos el *token* celular vino a brindar una mayor seguridad en las transacciones, sin embargo, los delincuentes mejoraron su operativa y continuaron "timando" a los clientes, razón por la cual, buscando una mejora continua en el 2009 se implementa el *token* llavero y el teclado virtual, entonces, gracias a ese esfuerzo del 2010 al 2015 no se reportaron timos por medio de internet *banking.*

Para el 2016 se empiezan a detectar casos a un nivel delictivo mayor, los delincuentes copiaban los sitios web del banco y mediante buscadores, utilizando enlaces pagados, guiaban a los clientes a páginas falsas. Definitivamente el grado de programación era diferente, se conocía qué se estaba haciendo y cómo se estaba haciendo.

Luego empezaron a utilizar las llamadas telefónicas, método efectivo hasta la fecha, ya que el concepto de "timo" adquiere un giro considerable y da paso aparición de un fenómeno llamado "ingeniería social". Entonces, nuestra función en cuanto a gestión de fraudes actualmente ha girado en torno a prevenir esta forma de adquisición de la información, mediante diferentes métodos de comunicación para tratar de informar a los clientes. Si el evento ya fue materializado pues se realiza el proceso correspondiente a los lineamientos de la institución

3. ¿Cuáles son las debilidades en ese proceso actualmente?

Definitivamente la ingeniería social que se le aplica a los clientes, ya que es lo más utilizado y el principal motivo de reclamos recibidos en nuestra dependencia. A pesar del esfuerzo realizado, el cliente sigue suministrando sus datos y su información bancaria ocasionando un reproceso en nuestras gestiones.

Diagnostico Operativo:

4. ¿Qué procedimientos, políticas o reglamentos internos se aplican?

La Contraloría de Servicios posee un procedimiento establecido por el banco, en el cual dicta los pasos a seguir cuando un cliente sufre de algún evento que preliminarmente se catalogue como fraude. El cliente debe presentar un reclamo administrativo, previo una denuncia ante el OIJ, adjuntar cierta información personal y esperar a que la gestión sea investigada por nuestra dependencia.

5. **¿Se aplican correcta y linealmente los procedimientos, políticas o reglamentos internos?**

   Totalmente, cada proceso es vital. Debemos estar conscientes de que la imagen del banco y la forma en que resuelva los casos que recibe son las principales fortalezas que se tienen, el fin es brindar seguridad a sus clientes en el uso de los diferentes canales electrónicos.

6. **¿Cómo debería ser la operativa según su opinión y experiencia en el proceso?**

   Cuando el cliente identifica que ha sido timado, la acción más rápida es llamar al banco, cuando esta llamada es atendida por el call center el ejecutivo debe identificar al cliente y posteriormente ir sistema por sistema bloqueando servicios, claro está, no todos los sistemas son administrados en el call center, razón por la cual una debilidad es precisamente que no existe un módulo centralizado de administración que brinde una respuesta rápida y precisa de los servicios que deben ser bloqueados para salvaguardar el patrimonio de los clientes. Es importante promover campañas informativas acerca de la ingeniería social aplicada a los clientes, no solo en Banco Nacional, sino en todo el sistema financiero nacional.

Diagnóstico Técnico:

7. **¿Con cuáles herramientas (infraestructura física o lógica, sistemas, aplicaciones) cuenta el departamento de seguridad para el registro de los fraudes?**

El departamento cuenta con el equipo físico necesario para el desempeño de las funciones, máquinas de escritorio, impresoras multifuncionales, etc. Por otra parte, a nivel de software se tiene acceso a los diferentes sistemas operativos y de consultas; estas consultas son realizadas mediante scripts en SQL cuando se requiere extraer de alguna base de datos, en fin, nuestra dependencia tiene acceso directo o indirecto a todos los sistemas que la institución tiene.

8. **¿Considera que el equipo actual (colaboradores y recurso tecnológico) cumple con los objetivos y alcances del departamento? ¿Qué mejoras consideraría?**

Podemos decir que sí, personalmente considero que algunas herramientas no funcionan como deberían o como se desearía ya que no existe tanta accesibilidad, quiero decir que se tiene que rastrear la información en las bases de datos. La institución actualmente debe hacer un esfuerzo con los sistemas ya que nunca se pensó, dentro de los requerimientos, solicitar módulos de reportaría que faciliten la búsqueda de información ante situaciones de auditoría, casas de investigación, entre otros.

El recurso humano siempre será importante y es necesario que el personal se pueda capacitar y que brinde ese soporte a los incidentes que se reciben día a día con el fin de disminuir los tiempos de espera dándole una mayor fluidez a las gestiones. Las oportunidades de mejora son pilares en nuestra gestión, debemos ir actualizando los procesos, ir adelante y concientizar a los clientes sobre el uso de los servicios electrónicos.

CONSENTIMIENTO

Fecha: 27- 11- 2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Joaquín Arias Ruiz
1-990-839
Nombre, cédula y firma del entrevistado

Firma del entrevistador

Anexo 2 Entrevistas, Dirección de Seguridad Informática

Entrevista

Banco Nacional de Costa Rica.

Dirección de Seguridad Informática.

Sr. Luis Fernando Alvarado Arce.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A) Explicación breve de objetivo general y específicos.

1. **Don Luis Fernando, para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.**

Tengo 33 años de servir en el Banco Nacional, de los cuales los últimos 27 los he desarrollado en el departamento de tecnología en diferentes departamentos: desarrollo, aplicaciones, arquitectura, y actualmente laboro como director de seguridad informática. Me corresponde llevar la administración general en temas de ciberseguridad del departamento.

2. **¿Cómo se realiza actualmente la administración de la parte de la seguridad informática?**

Nosotros estamos orientados a ver temas de: detección; atención; resolución de incidentes de ciberseguridad; análisis y posibles amenazas; nuevos métodos y soluciones para la gestión de la ciberseguridad; y también nos encargamos de identificar y recomendar la adquisición de nuevas soluciones

3. **¿Cuáles debilidades o dificultadas puede determinar en esa administración?**

Los retos más importantes que deben enfrentar los departamentos de ciberseguridad y no solo el Banco Nacional sino todas las entidades financieras, giran en torno al gran volumen de transacciones que actualmente se están realizando por diferentes medios electrónicos, estos servicios son 24/7 y los clientes hacen un uso constante de ellos. A esto debemos agregar que ahora las soluciones tecnológicas que ofrecen los bancos están basadas en infraestructuras híbridas, es decir, multiplataforma y también instaladas en

diferentes *Data Center*. Todo esto ha captado la atención por parte de los departamentos de ciberseguridad, ya que surgen entornos más complejos debido al volumen transaccional que se está manejando.

Diagnostico Operativo:

4. **¿Qué procedimientos o gestiones aplican ustedes día con día en la dirección de seguridad informática?**

   Se realiza una revisión constante de vulnerabilidades, validando que las mejores prácticas estén implementadas en los sistemas, además tenemos procedimientos que nos permiten tener una guía para validar las normativas y convertirlo en políticas para las diferentes áreas respectivas. También tenemos procedimientos que nos permiten primero, ayudar a los compañeros a detectar situaciones que no sean normales o fuera de las prácticas comunes, principalmente en el área de producción y segundo, guiarlos según las normas recomendadas.

   Parte de los procesos que estamos siguiendo en temas de certificación de calidad es que toda la documentación que utilizamos para este asesoramiento esté al alcance de los funcionarios de la institución, siendo las áreas más prioritarias el departamento de cajas, plataforma, ejecutivos de cuenta y jefaturas. Esto nos permite tener una mejora continua ya que los procesos son sometidos a una evaluación constante.

5. **¿Se aplican correcta y linealmente los procedimientos, políticas o reglamentos internos?**

Totalmente, se debe señalar que somos regidos u observados por entes reguladores internos y externos.

6. **¿Cómo debería ser la operativa según su opinión y experiencia en el proceso, buscando que sea más expedita?**

Existen 3 aspectos importantes que debemos seguir desarrollando en el banco:

a) La cultura de seguridad, entender que todos en el conglomerado tenemos una responsabilidad en temas de seguridad.
b) Trabajar fuertemente temas de automatización, como hemos hablado, el volumen transaccional que está manejando la institución es enorme, eso no se puede hacer por métodos anuales o herramientas de uso cotidiano, sino requerimos herramientas que procesen en tiempo real la información, definir o establecer tendencias, visualizar desviaciones, para luego tomar de decisiones oportunas.
c) Reforzar las estructuras operativas, tanto a nivel de cantidad como de preparación y obviamente de herramienta.

Diagnostico Técnico:

7. **¿Con cuáles herramientas cuenta el departamento de seguridad informática para la administración?**

El Banco toma muy enserio los temas de seguridad y desde hace bastante tiempo invierte cantidades importantes de recursos para contar con las herramientas que establezcan la mejores prácticas pero también se han venido incorporando las herramientas que requieren las demandas del negocio y las tendencias a nivel de amenazas y de buenas prácticas, el

banco cuenta con herramientas tradicionales como: *IPS; fireware; WAF; SOCK*; herramientas de monitoreo, de análisis de correos, de análisis de control de navegación, etc., lo que se considera como tradicional. También se han hecho inversiones en herramientas con aprendizaje de máquina y AI para lo que es análisis de datos de tal forma que toda la información esté dirigida tanto a reforzar la prevención y detección de fraudes como a la contención de incidentes.

8. **¿Considera que el equipo actual (colaboradores) cumplen con los objetivos y alcances del departamento?**

La seguridad no es un destino es necesariamente un proceso y todas estas herramientas tienen que ser administradas día a día, actualizadas en todas sus configuraciones para que estén acorde a las nuevas amenazas y los nuevos vectores de ataque, por ende, se tiene que estar en una mejora continua para cumplir con los objetivos principales de la institución.

El tiempo es muy relativo, en este momento se puede tener todos los elementos o herramientas, pero en 60 segundos ya estarán desactualizados y se deberá hacer modificaciones buscando otra solución o mejorar lo que se tiene.

9. **¿Qué mejoras o recomendaciones sugeriría usted enfocándose en la responsabilidad que tiene el cliente, el Banco y las diferentes dependencias en temas de seguridad informática?**

La seguridad es un trabajo en equipo en donde el banco tiene una enorme responsabilidad como prestatario del servicio, pero donde también el accionar de los clientes internos y externos es factor críticos para éxito, esto implica que todos los clientes

deben saber de seguridad, pero lo más importante que deben desarrollar sus labores y utilizar lo diferentes canales que tiene los bancos con suma prudencia y diligencia.

Todos los elementos de seguridad enfocados a los servicios están custodiados por los clientes, por ende, reiteramos que se deben de utilizar con mucha prudencia y una adecuada custodia, ya que en los últimos meses el principal medio utilizado por los delincuentes es la ingeniería social, por ende, se debe crear conciencia de que somos elementos esenciales dentro del esquema de seguridad.

CONSENTIMIENTO

Fecha: 30 - 11 - 2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado "***Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario***".

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Entrevista

Banco Nacional de Costa Rica.

Dirección de Seguridad Informática.

Sr. Cilliam Cuadra Chavarría.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. Explicación breve de objetivo general y específicos.

1. **Don Cilliam, para empezar, cuénteme de su experiencia profesional y de sus funciones en este departamento.**

   Mi experiencia profesional ronda los 25 años en temas de seguridad, he sido consultor y conferencista internacional siempre en temas de seguridad, además durante aproximadamente 12 años fui perito para el Banco Nacional en estemas de fraude, han sido varios años en función; tengo también varias certificaciones de ISACA y he pertenecido a grupos de esta organización

2. **¿Cómo se realiza actualmente la administración de la parte de la seguridad informática?**

   Tenemos un grupo de trabajo que se encarga de validar y verificar todos los controles en las áreas del banco en temas de seguridad, aplicativos como internet *banking*, canales electrónicos, aplicaciones, etc. Además, damos seguimiento a plataforma, cajas, servicios al cliente, cajeros automáticos, es decir, es nuestra función que todos aquellos medios electrónicos se estén ejecutando acorde a las mejores prácticas.

3. **¿Cuáles debilidades o dificultadas puede determinar en esa administración?**

Siempre se encontrarán oportunidades de mejora, los delincuentes pondrán en práctica nuevas formas de atacar y probar nuevos mecanismos, ya que tienen el tiempo necesario para efectuar y concretar el delito; en ese sentido es importante que nuestro departamento esté alerta ante esta situación y realizar las funciones de forma correcta. La mayor debilidad es no poder anticipar estos nuevos métodos, sin embargo, estamos en constante actualización acorde a las mejores prácticas de seguridad.

Diagnóstico Operativo:

4. **¿Qué procedimientos o gestiones aplican ustedes día con día en la dirección de seguridad informática?**

Se realiza una revisión constante de vulnerabilidades, validando que las mejores prácticas estén implementadas en los sistemas, además tenemos procedimientos que nos permiten tener una guía para validar las normativas y convertirlo en políticas para las diferentes áreas respectivas. También tenemos procedimientos que nos permiten primero, ayudar a los compañeros a detectar situaciones que no sean normales o fuera de las prácticas comunes, principalmente en el área de producción y segundo, guiarlos según las normas recomendadas.

Parte de los procesos que estamos siguiendo en temas de certificación de calidad es que toda la documentación que utilizamos para este asesoramiento esté al alcance de los funcionarios de la institución, siendo las áreas más prioritarias el departamento de cajas,

plataforma, ejecutivos de cuenta y jefaturas. Esto nos permite tener una mejora continua ya que los procesos son sometidos a una evaluación constante.

5. **¿Se aplica correcta y linealmente los procedimientos, políticas o reglamentos internos?**

   Eso es precisamente lo que se busca, que los procedimientos estandaricen la forma de operación.

6. **¿Cómo debería ser la operativa según su opinión y experiencia en el proceso, buscando que sea más expedita?**

   La inteligencia artificial es una tecnología que vendría a solucionar muchos de los procesos que actualmente requieren una gestión más lenta, un sistema o modelo: que brinde estadísticas de manera que los eventos sean identificados a nivel de transaccionalidad del cliente y que sean más analíticos y durante 24/7; que logre determinar comportamientos y acciones que puedan estar sujetas a intereses específicos con el fin de considerar que estén fuera de rangos de usabilidad y periodicidad para evitar pérdidas de patrimonio de los clientes

Diagnostico Técnico:

7. **¿Con cuáles herramientas cuenta el departamento de seguridad informática para la administración?**

El Departamento de Seguridad Informática guía a todas las áreas operativas, no está relacionado directamente con la operativa. Las asesoramos en el desarrollo de sus herramientas y mejora continua, por ende, se cuenta con un personal que se encarga de estas gestiones, por otra parte, cualquier modelo o sistema que ayude a fortalecer la administración de la seguridad será bienvenido.

8. **¿Considera que el equipo actual (colaboradores) cumplen con los objetivos y alcances del departamento?**

Es un tema de nunca acabar, cuántas personas se necesitan para determinada tarea. Proporcionalmente siempre se buscará alcanzar las mejores prácticas, el Banco Nacional ha buscado hacerlo, la mejor práctica actual relaciona la cantidad de inversión en tecnología con la inversión en seguridad. Contar con suficiente recurso humano siempre es importante, más si se quiere alcanzar un estándar internacional que está reconocido y para lo cual ya falta poco

9. **¿Qué mejoras o recomendaciones sugeriría usted enfocándose en la responsabilidad que tiene el cliente, el Banco y las diferentes dependencias en temas de seguridad informática?**

Como lo hemos venido conversando, las nuevas tecnologías y el uso de la inteligencia artificial en un modelo que potencialice: la analítica del comportamiento transaccional de los clientes; el uso responsable de la información bancaria por parte de los usuarios en las plataformas digitales; el compromiso de cada uno de los funcionarios del banco para mantener un sentimiento tanto de responsabilidad como de mejora de procesos, es la recomendación que haría en toda la administración y operativa de seguridad informática.

CONSENTIMIENTO

Fecha: 27-11-2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

William Cerdas
108280944
Nombre y firma del entrevistado

Firma del entrevistador

Anexo 3 Entrevistas, Plataforma de Servicios OP

Entrevista

Banco Nacional de Costa Rica.

Plataforma de Servicios.

Sr. Schneider Solano.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. Explicación breve de objetivo general y específicos.

1. Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.

Tengo 24 años de laborar para el Banco Nacional, he estado en diferentes oficinas realizando funciones operativas y administrativas, actualmente soy el jefe de la Plataforma de Servicios de la oficina principal.

Dentro de mis funciones básicamente me corresponde velar por que las cosas caminen de la mejor forma posible como un "director de orquesta", que el cliente sea bien atendido en cuanto al tiempo y a la forma, a pesar de que la estructura organizativa de la plataforma no es la misma que algunos años atrás. En resumidas cuentas es un tema de: gestión; seguimiento; de que el control interno se aplique para que el cliente salga satisfecho; de dar seguimiento a casos especiales de clientes o bien de colaboradores. Es una gestión administrativa pero si debo trabajar en temas operativos, estoy a disposición para lo que se necesite.

2. ¿Sabe usted qué es un timo o fraude informático y como afectan estos a los clientes?

Sí claro, el timo o fraude informático es buscar la manera de cómo convencer al usuario de que la herramienta suministrada por algún ente financiero es auténtica, y mediante una conversación de confianza, busco que me facilite toda la información que requiero para ingresar yo en sustitución de él.

Si el cliente brinda los datos de sus dispositivos de seguridad para ingresar a los servicios financieros, básicamente está imposibilitando que el banco actúe. El cliente debe ser responsable con sus datos, hacerse de la cultura de responsabilidad digital que le evite

entrar en un estado de vulnerabilidad. El problema no son las seguridades, sino la falta de cuidado del usuario al manejar la información para ingresar a los sistemas

3. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

En donde está publicado lo saco por deducción, ya que nunca he llegado a buscarlo, debe estar en la dirección de seguridad establecida cuál es el mecanismo para poder denunciar un fraude vía informática. El tramite es: el cliente se apersona, nos presenta la denuncia respectiva ante el OIJ, se le hace destrucción de la tarjeta, bloqueo de cuentas, se le quita el *token* y se le destruye, se le genera un *token* nuevo, se emite una nueva tarjeta, se procede a levantar las restricciones si el cliente tiene la voluntad de querer levantarlas.

No se puede proceder de oficio porque podría ser que el cliente ya no quiera tener relaciones comerciales con el banco, entonces nos emite una nota y junto con la denuncia se eleva a la gerencia de OP que es la dirección de zona y esta eleva el caso a la dirección de seguridad para que se inicie el análisis respectivo de la gestión, esa es la parte que yo conozco.

4. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente? Recomendaciones por parte del entrevistado.**

Debo conocer cuál es la manera efectiva de frenar el fraude desde el punto de vista de las herramientas que utilizamos nosotros, que quiere decir esto: que si un cliente se presenta con una situación lo primero que se debería conocer o hacer es eliminar el dispositivo *token* y si aplica, restringir las cuentas, eso como primeras acciones considerando que somos la

cara [del banco] ante el cliente en ese momento. A la vez evitamos entrar en temas de cómo lo estafaron, quién llamó o de dónde solicitaron la información, etc. Considero que el plataformista debe conocer cómo frenar el timo o fraude lo más ágil posible de manera que no siga causándole un perjuicio económico al cliente, posterior a eso, realizar la investigación que corresponde.

Como recomendación, se debe tratar de concientizar e intentar que el cliente interiorice cuáles son los dispositivos de vulnerabilidad que él tiene al usar una herramienta electrónica, con una sana administración de esos dispositivos se puede garantizar que el cliente no será víctima de fraude o estafa.

Además, se debe informar de manera continua todas las formas en las que los delincuentes pueden timar a las personas por medio de canales electrónicos, esto con el fin de que el cliente este en constante actualización y por ende más prevenido.

CONSENTIMIENTO

Fecha: 18 - 12 - 2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Schneider Solano Mora 1-0907-0080

Nombre, cédula y firma del entrevistado

Firma del entrevistador

BANCO NACIONAL DE COSTA RICA
Schneider Solano Mora
EMPL. 8101

Entrevista

Banco Nacional de Costa Rica.

Plataforma de Servicios.

Usuario: 1.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. Explicación breve de objetivo general y específicos.

1. Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.

Licenciado en Comercio Internacional, cursando actualmente el bachillerato en contaduría. Mi cargo es el de enlace y análisis de créditos, atender las solicitudes de crédito de los clientes, en cuanto a créditos de consumo, hipotecarios y tarjetas de crédito.

2. ¿Sabe usted que es un timo o fraude informático y como afectan estos a los clientes?

En palabras mías, un timo consiste en realizar un acto vandálico a una persona con tal de sacar provecho de ella, la mayor afectación que se presentan en estos casos son la perdida de dineros de las cuentas bancarias o bien tarjetas de crédito en transacciones no realizadas por el cliente.

3. ¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?

No, a grandes rasgos sé que se tiene que presentar al banco para presentar su debida queja y posteriormente que haga la investigación. Qué departamento se encarga de esto no sabría.

4. ¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente?

Conocimiento completo del cliente: a qué se dedica; qué productos mantiene con el banco; cómo son sus movimientos diarios, si se dan; cuáles son los movimientos fuertes en el año. Sobre todo, se debe de mejorar en el tiempo de respuesta por parte del banco.

CONSENTIMIENTO

Fecha: 5-12-2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado "***Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

DANIEL VARGAS VILLARREAL

1 1350842

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Entrevista

Banco Nacional de Costa Rica.

Plataforma de Servicios.

Usuario: 2.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. Explicación breve de objetivo general y específicos.

1. Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.

Mi experiencia profesional va desde ejercer la contaduría, ya que poseo una licenciatura y estoy incorporada al colegio respectivo, hasta ser cajera, planillera y plataformista, esto a lo largo de 9 años.

Mi cargo actual es ser plataforma, se atienden todos aquellos clientes que vienen a aperturar nuevos servicios, gestiones que otras oficinas no realizan porque no les gusta o no tienen la capacidad o conocimiento competente que deben de brindarles su jefatura o el banco como tal incentivando talleres o cursos de conocimiento, además de que el banco no estandariza los procedimientos a nivel de todas las zonas, si esto existe las jefaturas no logran ponerse de acuerdo para la aplicación de los mismos.

2. ¿Sabe usted que es un timo o fraude informático y como afectan estos a los clientes?

Claro que sí sé qué es un timo o fraude informático, a los clientes los afectan por dos razones, una porque el estafador es muy profesional, y dos porque los clientes son muy

confiados, el banco ha invertido cualquier cantidad de dinero en publicidad, mencionado y advirtiendo acerca de los timos que los estafadores utilizan, no se informan de lo que pasa en la actualidad y brindan información personal y de seguridad cuando se les ha dicho muchas veces que el banco no llama para pedir esa información.

Siempre he mantenido la certeza de que dentro del conglomerado banco nacional algunas personas filtran información de los clientes con cartera potencial, porque el estafador sabe muy bien a quien llamar ya que tiene dinero en su cuenta

3. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

Sinceramente nunca he visto la publicación del procedimiento como tal. Sé que el cliente debe hacer un manuscrito con lo sucedido, traer la denuncia del OIJ, estado de cuenta y cedula, entregar en la gerencia para su seguimiento; cabe mencionar que esto lo sé porque es lo que las jefaturas nos han indicado.

4. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente?**

Debe de haber un procedimiento en el mapa de procesos donde yo pueda corroborar como realizar la gestión y otra herramienta donde pueda visualizar el seguimiento de la denuncia, se acercan muchos clientes preguntando al respecto y lo único que podemos hacer el llamar a Noyman para que nos colabore en lo poco que él puede.

CONSENTIMIENTO

Fecha: 13-12-2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Rebeca Jerlén Guzmán / 114780784

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Entrevista

Banco Nacional de Costa Rica.

Plataforma de Servicios.

Usuario: 3.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario"

A. Explicación breve de objetivo general y específicos.

1. Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.

Tengo aproximadamente 15 años de laborar en este departamento (Plataforma de Servicios), las funciones son muy numerosas y en algunos casos existen tramites atípicos donde uno mismo debe buscar ayuda con otros compañeros para solventar las diferentes necesidades de los clientes. Sin duda alguna todos los días se aprende algo nuevo

2. ¿Sabe usted qué es un timo o fraude informático y cómo afectan estos a los clientes?

Desgraciadamente este tema es el pan de cada día y emocional y económicamente han sido ya muchos clientes afectados por casos de esta índole.

3. ¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?

El procedimiento como tal sí lo conozco debido a la práctica constante en los diferentes casos, sin embargo, ignoro la ubicación de tal publicación. Importante tomar en consideración que estos procedimientos son constantemente modificados y actualizados.

4. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente?**

Los aspectos fundamentales son conocer a fondo cada caso como tal ya que todos tienen diferentes formas o aspectos de haberse efectuado. Una gestión oportuna es bloquear el Internet *Banking*, reportar y cambiar las diferentes tarjetas de débito o crédito que el cliente posea y adicionalmente cambiar el *token* de seguridad.

CONSENTIMIENTO

Fecha: 11 - 12 - 2018

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Ronald Palma G. 1742077

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Anexo 4 Entrevistas, Banca Privada

Entrevista

Gerencia, Sucursales Digitales.

BAC San José.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario."

A. Explicación breve de objetivo general y específicos.

1. **Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.**

Desempeño la función de asistente gerencial en la Gerencia de Canales de Servicios específicamente en el Área de Sucursales Digitales (BAC). Mis función en el departamento es básicamente la administración general operativo-administrativo en el punto de sucursal que me encuentre, manteniendo todos los parámetros de cumplimiento de objetivos, supervisión de personal, seguimiento de proceso.

2. **¿Sabe usted qué es un timo o fraude informático y cómo afectan estos a los clientes?**

Claro, esto es una forma de fraude común en dónde se utiliza diferentes medios tecnológicos para realizarlos. Definitivamente afecta directamente al cliente comprometiendo su información confidencial y exponiéndolo a múltiples circunstancias de fraude (Financiero – Personal).

3. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

No trabajo directamente en esta Área de Fraudes. Sin embargo, mi equipo de trabajo que se relaciona directamente de al cliente; les es común ver este tipo de casos. En el Banco ya tenemos procedimientos establecidos en [los cuales] referimos estos casos por medio de sistemas determinados para que el cliente sea acompañado en el proceso y ejecutar todas

las gestiones necesarias para neutralizar el problema, realizar las investigaciones legales y a su vez las devoluciones implicadas.

4. ¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente? Recomendaciones por parte del entrevistado.

Para realizar una gestión oportuna son necesarias las evaluaciones principales del posible fraude:

- Número de cuenta / tarjeta implicada.
- Fechas de realización.
- Comercio afiliado / nombre empresa / página web/ qué giró el cobro.
- Montos globales por fraude.
- Referencia de cobros.

Luego, entendido que un oficial de servicio ingresa la gestión y la recibe un *backup* del área encargada que la atenderá y ejecutará la resolución correspondiente:

- Tener claro el proceso de la gestión, tanto en etapas como en tiempos de respuesta.

- Es importante comprender los diferentes escenarios comunes de reincidencia de fraudes (actividades normales vs fraudulentas) esto como reconocimiento para poder actuar en ayuda de cara al cliente. No está demás decir que las instituciones financieras deben estar a la vanguardia en los protocolos de seguridad electrónica.

CONSENTIMIENTO

Fecha: 9- 01 - 2019

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Nombre, cédula y firma del entrevistado

Firma del entrevistador

Entrevista

Atención al Cliente, Web Chat.

BAC San José.

Proyecto: "Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario.".

A. Explicación breve de objetivo general y específicos.

5. **Para empezar, cuénteme de su experiencia profesional, su cargo y funciones en este departamento.**

Funciones generales, atención al cliente por medio de web-chat, atiendo y soluciono las consultas de los clientes por medio de un chat que trabaja 24/7. Nuestro deber es tratar siempre de solucionar al cliente de forma rápida y veraz, ingresar gestiones para que otros departamentos estudien el caso más detalladamente en caso de que así sea necesario o bien ingreso de gestiones para solucionar al cliente su necesidad ya sea para devoluciones, liberaciones, desbloqueos, también guiar al cliente para que se autogestione por nuestras páginas, etc. En fin, ayudar al cliente con todas sus consultas de una forma clara para que así el cliente cierre de una forma satisfecha.

6. **¿Sabe usted qué es un timo o fraude informático y cómo afectan estos a los clientes?**

En mi opinión, sería el fraude que se realiza de forma electrónica, cuando se roba información del cliente para poder realizar compras, pagos, retiros de dinero con información que se obtuvo por medio de internet o de algún aparato inteligente. Esto afecta gravemente al cliente, ya que se le roba en caso de ser cuentas bancarias, el dinero propio del cliente, en caso de ser información de tarjetas de crédito, hace que el cliente vaya a pagar probablemente por algo que él/ella no solicitó o no obtuvo. Esto podría manchar al cliente ante muchas entidades bancarias o SUGEF, y en casos ya grabes, afectar al cliente haciéndolo pagar grandes cantidades de dinero por algo que no autorizó o bien quedar sin nada de dinero del que tenía ahorrado, por ejemplo.

7. **¿Conoce usted el procedimiento para atender un reclamo administrativo relacionado a un timo o fraude informático? ¿En dónde está publicado?**

Nosotros procedemos con una gestión de estudio legal llamada “contracargo” , esto básicamente se basa en el bloqueo del plástico (y así solicitar uno nuevo con nueva numeración) y haciendo el reclamo por medio de la gestión. Esto se envía a estudio por una cierta cantidad de días, ahora en 24h aproximadamente a muchos de los clientes se le reversa el dinero para que él no se tenga que hacer cargo del mismo, en caso de que el estudio falle a favor , se cierra el caso de forma exitosa, en caso de que no, el dinero se vuelve a debitar.

En este estudio se analizan muchos detalles de la transacción, se conversa con el personal del OIJ, se habla con el comercio, se solicitan cámaras para revisar, entre otras cosas. Este es el procedimiento al que tenemos conocimiento nosotros como servicio al cliente, no sabría más detalle, ya que de esto se encarga directamente el área de fraudes.

8. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente?**

Es importante conocer el proceso de la gestión para poder explicarla al cliente y que el mismo sienta confianza hacia uno durante este momento tan difícil para él. Tenemos que estar siempre actualizados con la información y con los cambios que se produzcan en las gestiones para el reclamo de fraudes.

Recomendaciones: no brindar información o fotos de sus cuentas o cédula a terceros; tener cuidado con las paginas por internet que utiliza e ingresa la tarjeta; no responder a correos sospechosos; siempre que haya alguna duda acerca de correos o mensajes que mejor contacte a su banco en primera instancia.

9. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente? Recomendaciones por parte del entrevistado.**

Nosotros procedemos con una gestión de estudio legal llamada “contracargo” , esto básicamente se basa en el bloqueo del plástico (y así solicitar uno nuevo con nueva numeración) y haciendo el reclamo por medio de la gestión. Esto se envía a estudio por una cierta cantidad de días, ahora en 24h aproximadamente a muchos de los clientes se le reversa el dinero para que él no se tenga que hacer cargo del mismo, en caso de que el estudio falle a favor , se cierra el caso de forma exitosa, en caso de que no, el dinero se vuelve a debitar.

En este estudio se analizan muchos detalles de la transacción, se conversa con el personal del OIJ, se habla con el comercio, se solicitan cámaras para revisar, entre otras cosas. Este es el procedimiento al que tenemos conocimiento nosotros como servicio al cliente, no sabría más detalle, ya que de esto se encarga directamente el área de fraudes.

10. **¿Cuáles aspectos considera usted que debe conocer para realizar una gestión oportuna y completa ante un reclamo de un cliente? Recomendaciones por parte del entrevistado.**

Es importante conocer el proceso de la gestión para poder explicarla al cliente y que el mismo sienta confianza hacia uno durante este momento tan difícil para él. Tenemos que estar siempre actualizados con la información y con los cambios que se produzcan en las gestiones para el reclamo de fraudes.

Recomendaciones: no brindar información o fotos de sus cuentas o cédula a terceros, tener cuidado con las páginas por internet que utiliza e ingresa la tarjeta, no responder a correos sospechosos, siempre que haya alguna duda acerca de correos o mensajes que mejor contacte a su banco en primera instancia.

CONSENTIMIENTO

Fecha: 4 - 01 - 2019

Autorizo al Sr. Abraham Cerdas Arce cédula 1-1340-0687, estudiante de la carrera de Licenciatura en Ingeniería Informática, a realizarme una entrevista para su proyecto de graduación, del cual tengo conocimiento y ha sido explicado por el entrevistador.

Acepto de igual forma, que las respuestas brindadas responden a mi experiencia y conocimiento personal sobre el tema de investigación y que las mismas serán anexadas al documento de tesis llamado ***"Modelo de perfil y comportamiento transaccional en la detección de fraudes en el sistema bancario".***

Katherine Moran Mora
113940876
Nombre, cédula y firma del entrevistado

Firma del entrevistador

8.1 REFERENCIAS BIBLIOGRÁFICAS

Alonso, R. (2017). *Phishing y otros 5 casos de fraudes bancarios en el 2017.* El Economista. Disponible en: https://www.eleconomista.com.mx/finanzaspersonales

Real Academia Española. (2018). *Diccionario de la Lengua Española*. Obtenido de http://dle.rae.es/?id=PTk5Wk1

Fierro, J. M. (3 de Diciembre de 2017). *Perfil transaccional: deber y reto para el sector financiero.* Portafolio. Disponible en: http://www.portafolio.co/economia/finanzas/perfil-transaccional-deber-y-reto-para-el-sector-financiero-512258

La Asamblea Legislativa de la República de Costa Rica. (9 de Noviembre de 2001). *La Gaceta N. 214 Ley 8148.* Disponible en: http://cpic.or.cr:81/moodle/pluginfile.php/43/mod_

/content/2/Ley%208148Adici%C3%B3n%20de%20art%20%20para%20reprimir%20y%20sancionar%20delitos%20inform%C3%A1ticos.%20La%20Gaceta%20N.%20214%209%20NOV.%202001.pdf

Pallares, F. (2014). *Desarrollo de un modelo basado en Machine Learning para la predicción de la demanda.* Disponible en://biblioteca.unitecnologica.edu.co/notas/tesis/0068209.pdf

Viscaya, R. (2018). *Deep Learnig para la detección de peatones y vehículos.* Atizapan de Zaragoza: Universidad Autonoma del Estado de Mexico. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/70995/tesisfinalRVC-ilovepdf-compressed%20%281%29.pdf?sequence=1&isAllowed=y

Julian, G. (2014). *Las redes neuronales: qué son y por qué están volviendo.* Disponible en: https://www.xataka.com/robotica-e-ia/las-redes-neuronales-que-son-y-p or-que-estan-volviendo

Vargas, Z. (2009). *La Investigación Aplicada: Una Forma de Conocer las Realidades con Evidencia Científica.* Obtenido de: https://revistas.ucr.ac.cr/index.php/educacion/article/viewFile/538/589

QuestionPro. (2018). *Qué es una investigación de campo.* Obtenido de https://www.questionpro.com/es/investigacion-de-campo.html

Sampieri. (2006). *Metodología de la Investigación.* Mexico: McGraw-Hill. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/70995/tesisfinalRVC-ilovepdf-compressed%20%281%29.pdf?sequence=1&isAllowed=y

Sampieri. (2006). *Metodología de la Investigación.* Mexico: McGraw-Hill. Obtenido de: https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf

Sampieri, H. (2010). *Metodología de la Investigación(5ta. ed.).* Mexico: McGrwa Hill. Obtenido de: http://ri.uaemex.mx/bitstream/handle/20.500.11799/70995/tesisfinalRVC-ilovepdf-compressed%20%281%29.pdf?sequence=1&isAllowed=y

Entrevista. (s.f.). Obtenido de https://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Curso_10/Entrevista_trabajo.pdf

Técnicas de Recolección de Datos. (s.f.). Disponible en: https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf

Rivero, D. B. (2008). *Metodología de la Investigación.* Shalom. Obtenido de: http://rdigital.unicv.edu.cv/bitstream/123456789/106/3/Libro%20metodologia%20investigacion%20este.pdf

Ruiz, F. P. (s.f.). *Diagrama de Flujo. Disponible en:* http://tecnicas-recoleccion-unach.blogspot.com/p/diagrama-de-flujo.html

Avilez, J. (s.f.). *Recolección de datos*. Disponible en: https://www.monografias.com/trabajos12/recoldat/recoldat.shtml#diagr

Saurabh. (s.f.). *Backpropagation - Algoritmo para entrenar una red neuronal*. Disponible en: https://www.edureka.co/blog/backpropagation/

Gartner. (2018). *IT GLOSARY*. Disponible en: //www.gartner.com/it-glossary/business-intelligence-bi

Banco Nacional de Costa Rica. (2018). Disponible en https://www.bncr.fi.cr/SitePages /Inicio.aspx

SUGEF. (2010). *ACUERDO SUGEF 12-10: NORMATIVA PARA EL CUMPLIMIENTO DE LA LEY Nº 8204* Disponible en : https://www.sugef.fi.cr/normativa/normativa _vigente/documentos/ SUGEF%2012-10%20(v13%20%2024may2017)%20SUGEF%20R-SGF-1318-2017.pdf

Mora, E. (2010). *Recolección de Datos*. Disponible en: http://erikandreamora.blogspot.com/

Banco Central de Costa Rica. (2017). *Aumentan casos de intentos de estafas bancarias.* Disponible en: https://www.bccr.fi.cr/seccion-comunicados-de-prensa/ComunicadosPrensa /Aumentan%20casos%20de%20intentos%20de%20estafas%20bancarias.aspx

La Teja. (27 de Julio de 2017). *BCR debe pagar a cliente estafado.* Disponible en: https://www.lateja.cr/nacional/bcr-debe-pagar-a-cliente-estafado/5T5UYBPURZEBZHVCSJDLI6OOP4/story/

Superintendencia Financiera de Colombia. (27 de Octubre de 2016). *Reseña de Jurisprudencia*. Disponible en://www.superfinanciera.gov.co/inicio/10087981

Salesforce. (2018). *¿Qué es Inteligencia Artificial?* Obtenido de salesforce: https://www.salesforce.com/mx/products/einstein/ai-deep-dive/

Rojas, P. (21 de Abril de 2014). *Los delitos informáticos son más comunes en Costa Rica de lo que se cree, según experto*. Disponible en: https://archivo.crhoy.com/los-delitos-informaticos-son-mas-comunes-en-costa-rica-de-lo-que-se-cree-segun-experto/tecnologia