

**UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS**



TRABAJO DE GRADO DE ESPECIALIZACIÓN EN:

**“AUDITORÍA FORENSE PARA LA DETECCIÓN DE FRAUDE
FINANCIERO ENFOCADO EN EL ROBO DE IDENTIDAD EN EL ÁMBITO
BANCARIO SALVADOREÑO”**

PRESENTADO POR:

ROCIO ESTEFANY ALVARADO MARAVILLA	L10802-1994
VILMA YESENIA CÁCERES GUEVARA	L10802-1994
NELSON GABRIEL SÁNCHEZ PUENTES	L10802-1994

SAN SALVADOR,

**ENERO 2022
EL SALVADOR,**

CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES CENTRALES

Rector : Msc. Roger Armando Arias Alvarado
Vicerrector Académico : PhD. Raúl Ernesto Azcúnaga López
Secretario General : Ing. Francisco Antonio Alarcón Sandoval

AUTORIDADES DE LA FACULTAD

Decano de la Facultad de Ciencias Económicas : Lic. Nixon Rogelio Hernández Vásquez
Secretario de la Facultad de Ciencias Económicas : Licda. Vilma Marisol Mejía Trujillo
Director de la Escuela de Contaduría Pública : Msc. Gilberto Díaz Alfaro
Coordinador General de Seminario de Graduación : Lic. Mauricio Ernesto Magaña Menéndez
Coordinador de Seminario de Procesos de Graduación de la Escuela de Contaduría Pública : Lic. Daniel Nehemias Reyes Lopez
Docente Director : Lic. Jorge Luis Martínez Bonilla
Tribunal Evaluador : Lic. Jorge Luis Martínez Bonilla
Lic. Daniel Nehemías Reyes López
Lic. Carlos Ernesto Ramírez

CC. A Directores de Escuelas, Coordinador General de Seminario de Graduación, Coordinador de Seminario de Proceso de Graduación

AGRADECIMIENTOS

Al concluir esta etapa de mi vida quiero extender un profundo agradecimiento a quienes me ayudaron a hacer posible este sueño, aquellos a quienes en todo momento estuvieron a mi lado y siempre han sido mi apoyo y fortaleza. Esta mención es especial para Dios por cada minuto que me otorga de vida, a mi madre, mi padre y mis hermanos, a mis compañeros y amigos. Muchas gracias a ustedes por demostrarme que “Solo con el corazón se puede ver bien, lo esencial es invisible a los ojos”. Mi gratitud también a la Escuela de Contaduría Pública, mi agradecimiento sincero al asesor de mi trabajo de graduación, gracias a cada docente quienes, con sus enseñanzas, constituyen la base de mi vida profesional y a mis compañeros de tesis por esta última aventura juntos. Gracias infinitas a todos.

Rocío Estefany Alvarado Maravilla

Agradezco primeramente a Dios por permitirme culminar esta etapa en mi vida y darme la sabiduría y entendimiento para superar cada dificultad que se presentó. Agradezco a mis padres por ser ese apoyo incondicional durante toda mi carrera y siempre motivarme a seguir adelante, a mi esposo por apoyarme y creer siempre en mí, a mis hijos y demás familia que me apoyaron durante todo este proceso, a mis compañeros de tesis, docentes y asesor que compartieron sus conocimientos y consejos conmigo.

Vilma Yesenia Cáceres Guevara

Doy gracias a Dios por haberme permitido llegar hasta el final de mi carrera, todo lo bueno proviene de Él. A mi familia, y en especial a mis padres por todo el esfuerzo que han hecho para darme lo necesario desde que comencé. A mis compañeros que a lo largo de esta etapa hemos coincidido para trabajar juntos. A mis amigos que me han brindado palabras de apoyo y motivación para seguir adelante y a todos los catedráticos de mi Facultad que nos han enseñado con esmero y dedicación y a todas las autoridades de la Universidad que hacen posible el cumplimiento de este sueño.

Nelson Gabriel Sánchez Puentes

ÍNDICE

RESUMEN EJECUTIVO	i
INTRODUCCIÓN	iii
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA Y MARCO TEORICO	
1.1 PLANTEAMIENTO DEL PROBLEMA	1
1.1.1 Situación actual del robo de identidad.	1
1.2 MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL	4
1.2.1 Antecedentes	4
1.2.2 Conceptos y definiciones	4
1.2.3 Generalidades de técnicas de auditoría forense	6
1.2.4 Técnicas forenses aplicadas a la auditoría forense	6
1.2.5 Generalidades de profesional ejerciente	7
1.2.6 Fraude.	8
1.2.7 Robo de identidad	9
1.2.8 Verificación de la identidad digital	12
1.2.9 Sistema bancario salvadoreño	14
1.2.10 Base técnica	15
1.2.10.1 NIEA 3000 (Revisada) Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica, marco internacional de encargos de aseguramiento y las modificaciones de concordancia de otras.	15
1.2.10.2 Normas internacionales de auditoría	16
1.2.10.3 Normas prudenciales del BCR	16
1.2.11 Base legal.	18
1.2.11.1 Ley especial contra los delitos informáticos y conexos.	18
1.2.11.2 Ley reguladora del ejercicio de la contaduría.	20
1.2.11.3 Ley de bancos	20
1.2.11.4 Código penal.	21
CAPÍTULO II: METODOLOGÍA DE LA INVESTIGACIÓN	
2.1 Enfoque y tipo de investigación	22
2.1.1 Tipo de estudio	22
2.2 Técnicas e instrumentos utilizados en la investigación	23
2.2.1 Técnicas	23

2.2.2	Instrumentos	23
2.3	Sujetos y objeto de estudio	23
2.4	Unidades de análisis, población y muestra	24
2.5	Variables e indicadores	24
2.5.1	Determinación de variables	24
2.6	Operacionalización de variables	32
2.7	Cronograma de actividades	33
2.8	Diagnóstico de la investigación.	34
CAPÍTULO III: CASO PRÁCTICO		36
3.1	PLANEACIÓN DE LA AUDITORÍA FORENSE	36
3.1.1	Introducción	36
3.1.2	Objetivos	37
3.1.3	Alcance	37
3.1.4	Riesgos	38
3.1.5	Información de la entidad	38
3.1.6	Áreas de la entidad:	39
3.1.7	Calidad en que actúa el profesional ejerciente	39
3.1.8	Sede	39
3.1.9	Definición y tipificación del hecho (tipo de fraude)	40
3.1.10	Causa	40
3.1.11	Afectado / ofendido / víctima	40
3.1.12	Presunto perpetrador / imputado / acusado	41
3.1.15	Flujograma del proceso	41
3.2	Antecedentes del caso	42
3.3	Normativa técnica para la ejecución de la auditoría forense	43
3.4	Estudio y evaluación del control interno	46
3.5	Evaluación de control interno: Área de negocios	48
3.6	Controles internos	51
3.7	Riesgos	52
3.8	Limitaciones	52
3.9	Planilla de Decisiones Preliminares	51
3.10	Programas de Auditoría	52
3.11	Análisis FODA de la entidad en El Salvador	55
3.12	Personal clave	56

3.13	Personal designado	56
3.14	Desarrollo del programa de auditoria forense	57
3.15	Presentacion de los resultados de la auditoria	82
4.	CONCLUSIONES	94
5.	RECOMENDACIONES	95
	BIBLIOGRAFÍA	96
	ANEXOS	

INDICE DE TABLAS

Tabla 1 “Ley especial contra los delitos informáticos y conexos”

Tabla 2 “Ley especial contra los delitos informáticos y conexos”

Tabla 3: “Ley reguladora del ejercicio de la contaduría pública”

Tabla 4: “Ley de bancos”

Tabla 5: “Código penal”

Tabla 6: “Operacionalización de variables”

Tabla 7: “Cronograma de actividades”

Tabla 8: “Aplicación de Normas Internacionales de Auditoría”

Tabla 9: “Aplicación de Normas Internacionales de Auditoría”

Tabla 10: “Cuestionario de control interno”

Tabla 11: “Programas de auditoría”.

Tabla 12: “Análisis FODA de la entidad en El Salvador”

INDICE DE FIGURAS

Figura 1: “Algunos ejemplos de cómo se explota el robo de identidad”

Figura 2: “Exposición al riesgo de fraude, FRAUD TREE”

Figura 3: “Flujograma del proceso”

Figura 4: “Líneas de defensa del sistema bancario”

Figura 5: “Planilla de decisiones preliminares”

RESUMEN EJECUTIVO

En los últimos años, la adopción de tecnologías en las operaciones financieras a nivel mundial ha propiciado el origen de diversos delitos en el medio electrónico, los usuarios de estas tecnologías crean sus identidades electrónicas para hacer uso de los servicios que prestan las entidades financieras y estos se convierten en potenciales víctimas de fraudes. A nivel nacional, la banca también se está modernizando y surge la necesidad de controlar la operacionalización de los servicios financieros y asimismo de detectar cualquier caso de fraude electrónico, de aquí el objeto de la investigación, se enfocó específicamente en el rol del auditor forense para los casos de fraude financiero a través del robo de identidad en la banca electrónica.

Las entidades afectadas por este tipo de fraude sufren daños económicos que impactan directamente la solvencia del negocio, además de los daños de imagen. Las variantes de estos delitos electrónicos también incluyen acciones directas contra personas que son engañadas para transferir dinero de sus cuentas a otras, de estafadores que las embaucan de múltiples maneras. Ante esto, los objetivos de este trabajo se enmarcan en proporcionar herramientas para fortalecer la capacidad profesional de los auditores forenses, mediante la conceptualización del delito, normativa técnica y legal, y técnicas de auditoría aplicables a los casos de fraude financiero por robo de identidad en la banca electrónica.

Esta investigación es de naturaleza cualitativa, ya que se estudia desde las causales del problema, su sistema de relaciones y su estructura dinámica hasta las propuestas de soluciones desde la perspectiva de los auditores forenses involucrados en casos de fraude financiero a través del robo de identidad. El tipo de estudio que se realizó fue el hipotético-deductivo, el

cual procede de una verdad general hasta llegar al conocimiento de verdades particulares o específicas.

Como resultado de esta investigación se proponen una serie de técnicas que el auditor forense podrá aplicar en determinados casos, se utilizó la entrevista como recurso de consulta a un profesional ejerciente para determinar las áreas de fortaleza y las necesidades que estos tienen para el mejoramiento de sus funciones en el ámbito. Se desarrollo un caso práctico con el cual se aportó un modelo de programa de auditoría para la detección de fraude en un caso de robo de identidad en la banca electrónica salvadoreña.

Se concluyó que todos los profesionales ejercientes reconocen que el robo de identidad es un riesgo existente en la banca electrónica del Sistema Bancario Salvadoreño, el cual presenta sus fallas, y que el auditor forense, con las herramientas y técnicas indicadas, juega un rol importante para la prevención y detección de fraudes a través de estos medios.

En el presente documento queda a disposición una fuente bibliográfica para todo profesional y estudiante del área de auditoría que puede servir para sus prácticas profesionales y para desarrollar sus actividades de auditoría.

INTRODUCCIÓN

El robo de identidad es un tipo de fraude financiero que ha aumentado a través de los años, el uso de la internet a propiciado el surgimiento de la identidad digital que se encuentra constituida por datos personales sensibles que pueden incluir claves de acceso a cuentas bancarias o diversas plataformas electrónicas. Los usuarios de servicios financieros cada día realizan más transacciones por medios digitales como lo es la banca en línea, utilizan sus tarjetas de crédito y tarjetas de débito como método de pago las cuales contienen una gran cantidad de datos personales, cada dato es una mina de oro para los estafadores, ya que una vez que obtiene esa información puede ser utilizada para un fraude sin el usuario darse cuenta en el momento.

El robo de identidad es uno de los delitos más frecuentes en el sistema financiero, esto conlleva a la necesidad que los profesionales ejercientes de la contaduría pública y auditoría contribuyan a esclarecer este tipo de delitos dentro de estas entidades. Como resultado de esa necesidad, se ha procedido a la realización de esta investigación; la cual se presenta en tres capítulos principales.

El capítulo I describe el planteamiento del problema, la caracterización donde se resaltan aspectos encontrados entorno a la problemática y la formulación del mismo, los objetivos de la investigación y el marco teórico, conceptual técnico y legal que sustenta y limita el estudio de la problemática, analizando los antecedentes y situación actual, las principales definiciones para comprender el contexto de la investigación, así como las generalidades de esta temática. Además, se presenta la normativa técnica y legal que es aplicable a esta área de especialización.

En el capítulo II se desarrolla la metodología de la investigación que comprende las estrategias, métodos y técnicas utilizadas en el proceso investigativo, el enfoque y tipo de investigación, los sujetos y objeto de estudio, las unidades de análisis, los instrumentos utilizados para la recopilación de información, las variables e indicadores, la operacionalización de las variables, el cronograma de actividades, el análisis de los resultados obtenidos, concluyendo con el diagnóstico de la investigación.

En el capítulo III se encuentra la propuesta de solución a la problemática basada en un modelo de auditoría forense para la detección de fraude financiero a través de robo de identidad en el sistema bancario, la cual contiene los elementos, programas y procedimientos que se deben de considerar para la realización de esta actividad.

Finalmente se presentan las conclusiones y recomendaciones de la investigación.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA Y MARCO TEORICO

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Situación actual del robo de identidad.

Es cierto que el robo de identidad no es un nuevo tema, pero sí es relevante saber cómo evolucionan los canales y técnicas de engaño que usan los delincuentes sobre las personas

El robo de identidad creció considerablemente durante la pandemia surgida en 2020, al incrementarse las compras en línea las personas realizan más transacciones utilizando sus tarjetas de crédito y débito como método de pago exponiendo sus datos ante páginas falsas que buscan robar información.

Durante los últimos meses las entidades bancarias se han esforzado por simplificar la banca en línea y agilizar los pagos de los clientes ante los cambios que ha traído la pandemia del COVID-19, pero es en este momento en que más personas están demandando hacer compras y pagos en línea, por lo que se debe cuidar más celosamente la información, pues el fenómeno que está ganando terreno hoy en día es el robo de identidad y los fraudes en línea.

Los defraudadores ponen su atención en un objetivo que, si no se toman las medidas preventivas, puede resultarles más sencillo robar la información del cliente. Las formas más comunes que están utilizando son:

- **A través de llamadas:**

Una de las formas más comunes de fraude es por medio de llamada telefónica. Consiste en un supuesto aviso del banco, que informa sobre un problema informático o movimientos inusuales en sus cuentas o tarjetas.

La persona al otro lado de la línea con frecuencia utiliza similar protocolo de atención al cliente y en algunos casos hasta ponen de fondo música o mensajes publicitarios del banco.

La trampa consiste en que por “su seguridad” le pedirán que brinde sus datos de acceso bancarios, así como credenciales para supuestamente confirmar su identidad y evitar el robo, cuando realmente el robo está en proceso. Se han reportado casos en los que incluso realizan una llamada tripartita entre el cliente, un supuesto agente del banco y un tercero.

Si se recibe una llamada de este tipo, lo mejor es terminar la comunicación y de inmediato contactar a su banco a través del número oficial de atención al cliente, y notificar el incidente.

- **Por correo electrónico:**

Otro de los fraudes en línea más comunes es por medio de correo electrónico, donde los defraudadores pueden recrear sitios web parecidos a una entidad bancaria y enviar el enlace a su dirección de correo que en algún momento pedirá sus datos de acceso e información personal.

Por eso no se debe abrir cualquier enlace que llegue por correo, sino que se debe verificar antes, pues, aunque no llegara a introducir información delicada, también podría ser un enlace de descarga a programas maliciosos que dan acceso a controlar dispositivo (celular, computadora o tableta) y así obtener la información que necesitan saber para sustraer dinero de las cuentas.

- **Lo más reciente: fraudes a través de redes sociales.**

Las promociones o sorteos desde perfiles que aparentan ser de instituciones bancarias, e incluso pagando publicidad, han sido identificadas recientemente.

Otra forma de fraude que está haciéndose popular, sobre todo entre micro y pequeñas empresas o personas que venden directamente a través de las redes sociales es cuando son contactados por un supuesto comprador, generalmente con acento extranjero, muy decidido y que ya hasta hizo listado del pedido.

A la hora de realizar el pago, por medio de una transferencia electrónica, aseguran tener inconvenientes y haber contactado al banco para verificar y hacen una comunicación entre las tres partes para “resolver el inconveniente”, pero realmente quieren que la persona brinde información personal para acceder a su banca en línea y correo electrónico.

Los perfiles oficiales de entidades financieras usualmente tienen un check de verificación de la cuenta, lo que evidencia que realmente es quien dice ser.

El robo de identidad se trata de un fenómeno que saca provecho de las debilidades y descuidos de los usuarios sobre su información. La mayoría de las personas suelen abrir cuentas de correos electrónicos, a las cuales acceden desde diversos dispositivos sin tomar acciones de precaución. De acuerdo con estimaciones, al menos el 36% de las empresas a nivel mundial han reportado haber sufrido de robo de identidad, lo que representa un grave riesgo de seguridad.

Tan sólo en el último año, el cibercrimen se ha incrementado en más del 37% a nivel mundial. De hecho, en todas sus variantes, ya ocupa una tercera parte de la totalidad de ofensas en el mundo, sólo detrás de delitos como el robo de propiedad, corrupción, entre otros.

1.2 MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL

1.2.1 Antecedentes

La Auditoría forense surge con los intentos de detectar y corregir el fraude en los estados financieros, pero con el pasar del tiempo ha ido aumentando su campo de trabajo. Esta auditoría parte del supuesto que existe la intención de dolo, lo cual le obliga a aplicar un conjunto de técnicas específicas como herramientas que le permitan la detección y análisis de la información, mismas que ayudan a desarrollar de una manera más efectiva la detección de fraudes u otro ilícito que se esté dando dentro de la institución.

El robo de identidad es el fraude de más rápido crecimiento en el mundo. Hasta no hace mucho tiempo, cuando un ladrón robaba una billetera o una porta documentos, el dinero era lo único que pretendía. Con el tiempo, los datos de los documentos de identidad como por ejemplo, la tarjeta de crédito, la tarjeta de débito, los cheques, o cualquier otro documento que contenga datos personales, han pasado a ser el objetivo de muchos timadores.

En el transcurso de pocas horas, esta información a veces se divulga al hacer transacciones en persona, por teléfono y en línea, al efectuar la compra de productos y de servicios. Si esta información confidencial es simplemente escuchada por un delincuente u obtenida por cualquier otro procedimiento, podría utilizarse para suplantar la identidad financiera de esa persona, y realizar muchas operaciones perjudiciales para el titular

1.2.2 Conceptos y definiciones

Dentro del robo de identidad se manejan muchos conceptos técnicos, mencionamos algunos de ellos para ir profundizando en el tema.

Factores de riesgo de fraude. Son hechos o circunstancias que indican la existencia de un incentivo o elemento de presión para cometer fraude o que proporcionan una oportunidad para cometerlo;

Ciberriesgo, riesgo cibernético o de ciberseguridad. Posibles resultados negativos derivados de fallas en la seguridad de la infraestructura tecnológica o asociados a ataques cibernéticos;

Ciberseguridad. Desarrollo de capacidades técnicas para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio y que es esencial para la operación de la entidad;

Confidencialidad. Propiedad de la información por la cual se le considera accesible sólo a aquellos debidamente autorizados y solo para los fines específicos y expresamente delimitados;

Factor de autenticación. Información utilizada para verificar la identidad de un servicio o una persona;

Base de datos. Programa capaz de almacenar gran cantidad de datos, relacionados y estructurados, que pueden ser consultados rápidamente de acuerdo con las características selectivas que se deseen;

Skimming. (copia de la tarjeta con un dispositivo de lectura de datos) En los últimos tiempos, la manipulación de cajeros automáticos para obtener información de la tarjeta de crédito de la víctima y sus códigos de acceso se ha convertido en un importante motivo de preocupación;

Peska o pharming. El término “peska” se utiliza para describir los actos con los que se trata de inducir a la víctima mediante técnicas de ingeniería social a revelar datos personales o confidenciales.

Phishing. Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios

1.2.3 Generalidades de técnicas de auditoría forense

Las técnicas de auditoría forense aplican los conocimientos y métodos a fin de identificar y comparar evidencias materiales asociadas a hechos presuntamente delictivos.

Dado que la auditoría forense es investigativa y busca establecer cómo se realizó un fraude y quienes fueron los implicados, por lo que hace uso de técnicas especializadas como medio de comprobación de evidencia y compararla con los hechos del delito, ayudando así a que la auditoría forense sea más certera al momento de detectar el origen y la ubicación de la responsabilidad de un fraude.

1.2.4 Técnicas forenses aplicadas a la auditoría forense

- **Documentología.** Esta técnica hace referencia a determinar la autenticidad o falsedad de documentos como títulos valores (cheques, tarjetas plásticas débito y crédito, letras de cambio, pagarés, entre otros) de identificación personal, impresiones de sellos, derechos de autor, documentos anónimos, entre otros.
- **Grafología.** Esta técnica hace referencia a establecer la autenticidad o falsedad de los escritos mediante la imprecisión manuscrita en documentos públicos y privados como, por ejemplo: escrituras públicas, recibos, facturas, certificados entre otros.
- **Informática forense.** Esta técnica hace referencia a obtener y presentar datos que hayan sido procesados electrónicamente y almacenados en soportes informáticos.
- **Técnica de entrevista/interrogatorio.** Esta técnica es un proceso de investigación estructurado que involucra tres etapas principales: análisis de los hechos, la entrevista de investigación y solo cuando procede, el interrogatorio.

1.2.5 Generalidades de profesional ejerciente

El auditor forense es un profesional valioso y altamente necesario en nuestra actual sociedad, es uno de los llamados a combatir la corrupción financiera, pública y privada.

Generalmente se requieren de los siguientes atributos para un auditor forense:

- Una mentalidad investigadora
- Mente inquisitiva y alerta
- Una comprensión de motivación
- Creatividad para poder adaptarse a las nuevas situaciones.
- Juicio profesional maduro y audaz.
- Orientado a la detección e investigación de fraude.
- Conocer las técnicas de redacción de informes.

Su juicio profesional basado en principios éticos, conocimientos generales y técnicos se enmarca en:

- Probidad moral.
- Responsabilidad intelectual.
- Independencia de criterio.
- Lealtad al servicio.

Habilidades del auditor forense:

- Capaz de identificar problemas financieros y operativos.
- Conocimiento de técnicas investigativas.
- Conocimiento de evidencia
- Interpretación de información financiera
- Experto en reconocer riesgos y evaluar controles.

- Presentación de hallazgos.
- Habilidades de comunicación, persuasión y una habilidad de comunicar en condiciones de ley.
- Habilidades de mediación y negociación (UNIVERSIDAD DE EL SALVADOR et al., 2009, #)

1.2.6 Fraude.

Un acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la utilización del engaño con el fin de conseguir una ventaja injusta o ilegal.

El fraude es un riesgo que existe en todo tipo de organizaciones por lo que se hace preciso concederle la grave importancia que tiene. Donald R. Cressey quien en 1961 expuso su conocida teoría respecto a los condicionantes para que se materialice el fraude, debiendo coexistir para ello tres situaciones:

1º) **Motivación** (incentivo, presión). Cuando la Administración u otros empleados tienen un estímulo o presiones que les aportan razones justificativas para cometer fraudes.

2º) **Poder** (oportunidad). Serían las circunstancias que facilitan las posibilidades de perpetuar fraudes (por ejemplo, la ausencia de controles, controles ineficaces, o la capacidad de la administración para abrogar los controles).

3) **Racionalización** (actitud). Cuando las personas son capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto. (Universidad politécnica salesiana et al., 2014)

1.2.7 Robo de identidad

La identidad la constituyen datos personales como el nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y de seguridad social; números de tarjeta de crédito y de cuentas bancarias; nombres de usuario y contraseñas; incluyendo información financiera o médica, así como cualquier otro dato que permita identificar a una persona. (Condusef Oficial, 2016). Este es un problema que en los últimos años se ha incrementado con el uso de Internet y el comercio electrónico.

Existen varias categorías de delitos de robo de identidad y la mayoría de ellos se clasifican en los siguientes cuatro tipos principales:

Robo de identidad delictiva:

Hace alusión a una situación en la cual alguien asume su identidad con el fin de evitar consecuencias jurídicas. Por lo general, se da cuando una persona facilita información falsa a la policía al ser detenida. Los ladrones que perpetraron esta clase de robo pueden poseer documentos oficiales expedidos por el Gobierno que hayan obtenido de forma fraudulenta con los datos de su víctima o a lo mejor solo tienen un documento falso.

Robo de identidad médica:

Es cuando alguien recibe un tratamiento médico que iba destinado a otra persona, el riesgo es especialmente elevado en países que cuentan con sistemas sanitarios privados, como en Estados Unidos, luego cuando la víctima acude a solicitar atención médica, puede encontrarse con la denegación del tratamiento pues ya ha sido usado.

Robo de identidad infantil:

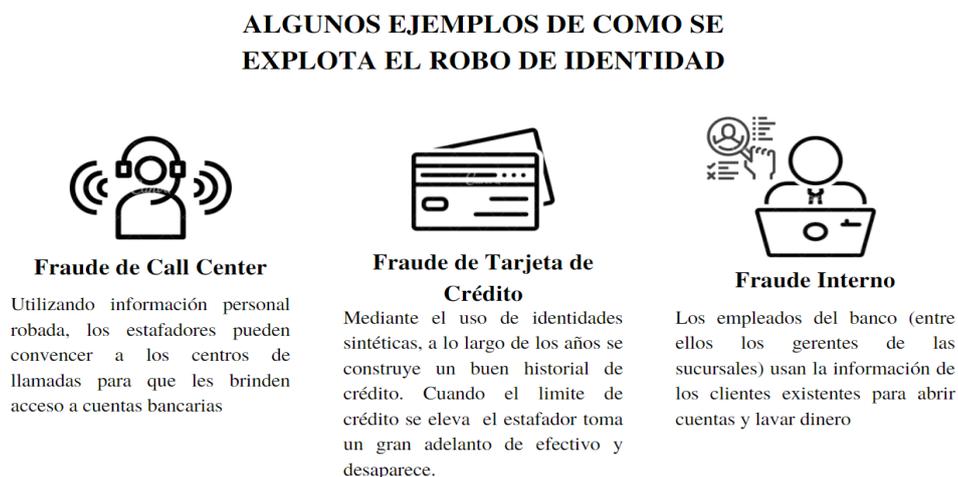
Ocurre cuando alguien roba y utiliza la identidad de un niño o una niña, en estos se ven involucrados los sistemas de acogida familiar, ya que son muchas las personas que tienen acceso a la información de los niños.

Robo de identidad financiera:

Es el tipo más común y sencillo, ocurre en el momento en que alguien emplea la información de una víctima para conseguir dinero por medios fraudulentos. También es uno de los tipos de robos de identidad más perjudiciales, pues supone una pérdida directa para la víctima. Algunas de estas figuras son las siguientes:

- Fraude de adquisición de cuenta.
- Fraude con tarjetas de crédito o débito.
- Estafas y robo de identidad para personas mayores.
- Fraude hipotecario.
- Fraude de compra online.
- Robo de identidad fiscal.

Figura 1: “Algunos ejemplos de cómo se explota el robo de identidad”



Fuente: (Lurie, 2018)

La variedad de tácticas utilizadas por los ladrones de identidad son diversas y pueden ir desde métodos tradicionales como el robo de la correspondencia hasta prácticas de alta tecnología tales como ataques cibernéticos masivos a bancos, cadenas de tiendas y otras entidades.

Las personas que se dedican a esta práctica fraudulenta en ocasiones dicen representar a instituciones de gobierno, solicitando datos personales o financieros; de igual manera, afirman llamar de bancos, empresas de servicios públicos o empresas de tecnología para obtener datos de las potenciales víctimas o bien envían correos electrónicos de suplantación de identidad ("phishing") vinculados a que infectan los equipos computacionales u otros dispositivos con programas malignos que recolectan información.

Al disponer de dicha información, los ladrones pueden usarla para efectuar operaciones por medio de tarjetas de crédito sin que la víctima pueda evitarlo, pueden pagar tratamientos médicos, efectuar declaraciones y pago de impuestos e incluso gestionar préstamos a nombre de la víctima. Los costos del robo de identidad no se limitan a poseer sólo una expresión monetaria sino, implican además destinar mucho tiempo para el rastreo de cuentas falsas, reparar el crédito dañado y, además, restablecer la propia identidad ante entidades financieras e instituciones de gobierno.

Estas prácticas suponen la existencia de dos sujetos, el titular perjudicado de los casos es el sujeto pasivo y quien realice los actos fraudulentos es el sujeto activo. Las personas que cometen el robo de identidad son aquellas que poseen ciertas características ya que tienen habilidades para el manejo de sistemas informáticos y otros tipos de habilidades sociales y que generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, con el tiempo se puede comprobar que estos tipos de actos sean muy diversos ya sea el caso de

un experto que ingresa en un sistema informático, o bien un empleado de una institución financiera que desvía fondos de las cuentas de los clientes.

1.2.8 Verificación de la identidad digital

La verificación de la identidad siempre ha sido un punto clave para las empresas que necesitan cumplir con las regulaciones KYC (Know Your Customer) y mitigar el riesgo de fraude en la aplicación durante la incorporación de clientes en persona. Esta tiene lugar cuando un cliente produce documentos de identificación válidos durante el proceso de incorporación, si esta fuera para clientes remotos, las instituciones financieras han recurrido a la verificación de identidad digital para poder incorporar a los clientes remotos de forma segura y conforme a las normas.

La mayoría de las Instituciones Financieras ya han comenzado este proceso de digitalización para los procesos de apertura de cuentas, se estima que el 85% proporcionan alguna forma de apertura de cuentas digitales a los clientes.

Previamente a la actual pandemia, los presupuestos asignados a los programas de apertura de cuentas digitales casi se habían duplicado en tamaño. Así que el deseo de digitalizar ya existía, junto con el respaldo financiero, aun cuando los requisitos básicos para la digitalización siguen siendo los mismos, las instituciones financieras tienen ahora un motor más apremiante que es la velocidad de comercialización. Con anterioridad al Covid-19, muchas instituciones financieras habían digitalizado parcialmente los procesos de los clientes, ejemplo de ellos es que; un cliente podía iniciar una solicitud de préstamo en línea y luego finalizar con una visita en persona en una sucursal para mostrar sus documentos de identidad. Estos escenarios mixtos contribuyeron en cierta medida a satisfacer la demanda de los consumidores de acceso en línea a los productos financieros.

Actualmente las instituciones financieras que quieren adquirir nuevos clientes deben averiguar cómo embarcar plenamente a un cliente de forma físicamente distante, esto implica añadir la verificación de identidad digital a sus capacidades en línea. Cuanto más rápido puedan alcanzar este objetivo, mejor podrán adaptarse a una situación en la que los servicios digitales son una necesidad además de una preferencia.

Precisos requisitos de seguridad, confidencialidad y cumplimiento en la verificación de la identidad digital.

Los clientes que pretenden poder abrir una cuenta o acceder a los servicios bancarios con la mínima fricción, pero también quieren sentirse seguros de que existe el nivel de seguridad adecuado para proteger tanto su cuenta como su identidad. La adopción de la verificación de la identidad digital debe incluir una precavida consideración de todos los requisitos de seguridad, antifraude, privacidad de los datos y cumplimiento, siendo la seguridad de los datos y la cuenta del cliente la principal preocupación.

Toda persona que participe en programas de trabajo destinados a la digitalización de un proceso de apertura de cuenta será muy consciente de los numerosos requisitos que deben cumplirse cuando se desarrollen las funcionalidades internamente o se seleccionen proveedores externos para proporcionar determinadas capacidades.

Los siguientes requisitos son recomendables para la implementación de nuevas soluciones:

- Verificación de identidad a través de canales, ya sea online, móvil, sucursal, call-center y cara a cara con los asesores.
- Geografía, si es compatible con las identificaciones de documentos en los países, estados y provincias en los que se realizan los negocios.

- Gestión del riesgo y el fraude, las transacciones remotas y sin rostro son más susceptibles de fraude, se debe gestionar adecuadamente el riesgo de fraude y ayudar activamente a reducir el fraude en las aplicaciones.
- Garantía de calidad y diligencia debida, es recomendable que los procesos sean automatizados
- Eliminación de los procesos en papel y captura electrónicamente la intención/consentimiento de la firma y los rastros de auditoría.
- Exigibilidad y cumplimiento legales, es el acuerdo resultante entre el cliente y la institución financiera legalmente exigible, el cual debe cumplir con el proceso de verificación de identidad con las normas pertinentes.
- Seguridad de la infraestructura, los dispositivos y las aplicaciones, la solución/proveedor asegura contra los ciberataques y los agentes malintencionados.

1.2.9 Sistema bancario salvadoreño

El principal papel de un banco consiste en guardar fondos ajenos en forma de depósitos, operaciones denominadas de pasivo. Los bancos cobran una serie de comisiones por los distintos servicios que ofrecen a sus clientes; sin embargo, puesto que el banco puede disponer del ahorro del depositante, remunera a este último mediante el pago de un interés. Se puede distinguir varios tipos de depósitos como, cuentas corrientes en las que el cliente cede al banco unas determinadas cantidades para que éste las guarde, pudiendo disponer de ellas en cualquier momento. Los bancos ofrecen cuentas de ahorro, que también son depósitos a la vista, es decir, que se puede disponer de ellos en cualquier momento. Los depósitos y reintegros se realizan y quedan registrados a través de una tarjeta de ahorro, que tiene carácter de documento financiero. La disponibilidad de este tipo de depósitos es menor que la de las cuentas corrientes puesto que obligan a recurrir a la entidad bancaria para disponer de los fondos, mientras que

las cuentas corrientes permiten la disposición de fondos mediante la utilización de cheques y tarjetas de crédito. También están los denominados depósitos a plazo, en los que no existe una libre disposición de fondos, sino que éstos se recuperan a la fecha de vencimiento. Existen también los denominados certificados de depósito, instrumentos financieros muy parecidos a los depósitos o cuentas a plazo fijo; la principal diferencia viene dada por cómo se documentan. Los certificados se realizan a través de un documento escrito intercambiable, es decir, cuya propiedad se puede transferir y negociar en los mercados financieros. Los bancos, con estos fondos depositados, conceden préstamos y créditos a otros clientes, cobrando a cambio de estas operaciones (denominadas de activo) otros tipos de interés. Estos préstamos pueden ser personales, hipotecarios o comerciales. La diferencia entre los intereses cobrados y los intereses pagados constituye la principal fuente de ingresos.

1.2.10 Base técnica

1.2.10.1 NIEA 3000 (Revisada) Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica, marco internacional de encargos de aseguramiento y las modificaciones de concordancia de otras.

Tiene como propósito establecer los principios básicos y los procedimientos esenciales, así como proveer guías a los contadores públicos para la ejecución de contratos de aseguramiento diferentes de auditorías o revisiones de la información financiera. Esta Norma comprende los trabajos para atestiguar con seguridad razonable y los trabajos para atestiguar con seguridad limitada.

1.2.10.2 Normas internacionales de auditoría

Estos estándares o reglas profesionales que tratan sobre las responsabilidades del auditor al realizar la inspección o auditoría financiera de la información suministrada por una entidad económica, a pesar de no estar diseñadas específicamente para la auditoría forense, resultan de mucha utilidad al analizar la responsabilidad de un auditor en la detección de fraudes, la planificación de auditoría, la evaluación y respuesta a los riesgos de auditoría y las evidencias, entre otros aspectos importantes. Su rol es constituir un soporte técnico para lo estatuido en la NIEA 3000.

1.2.10.3 Normas prudenciales del BCR

La regulación prudencial tiene por objeto fortalecer los niveles de solvencia, mejorar la calidad de capitales y las prácticas de gestión de riesgos de las entidades del sistema financiero y en especial de los bancos, esto mediante la adopción de mejores estándares. Esta regulación se refiere a una serie de estándares mínimos que se les impone a las entidades de intermediación financiera con el fin de practicar una regulación más eficiente y promover prácticas financieras saludables. Las normas prudenciales que se utilizaron en la investigación son:

- NRP-23 Normas técnicas para la gestión de la seguridad de la información.
Hace referencia a los criterios mínimos que se deben establecer para la gestión de la seguridad de la información y la ciberseguridad de la institución que estén acordes a las mejores prácticas internacionales
- NRP-20 Normas técnicas para la gestión integral de riesgos de las entidades financieras.

Decreta las disposiciones mínimas que deben de observar las instituciones para la gestión integral de riesgos de conformidad con las leyes aplicables.

- NRP- 15 Normas técnicas de auditoría interna para los integrantes del sistema financiero. Establece las disposiciones mínimas que deberán considerar las entidades para el ejercicio de la auditoría interna y fomentar la adopción de procedimientos y técnicas de trabajo con un enfoque de auditoría con base en riesgos
- NPB4-50 Normas para la gestión de riesgo operacional de las entidades financieras. Proporciona lineamientos mínimos para una adecuada gestión de riesgos operacionales y criterios para la adopción de políticas y procedimientos relacionados con el desarrollo de métodos para la gestión de riesgos operacionales.
- NPBT-06 Normas técnicas temporales sobre medidas de Ciberseguridad e identificación de los clientes en canales Digitales. Establece reforzar las medidas de ciberseguridad en los sistemas informáticos de las entidades financieras mediante los cuales se recopila, procesa, transmite y almacena la información de las entidades financieras, así como la implementación de medidas para la correcta identificación de los clientes.

1.2.11 Base legal.

1.2.11.1 Ley especial contra los delitos informáticos y conexos.

Esta ley tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas.

Tabla 1 “Ley especial contra los delitos informáticos y conexos”

Título I. Disposiciones generales		
No. Art.	Precepto	Aplicación auditoría forense
Art 1.-	Objeto de la ley	Detección de conductas delictivas desarrolladas a través de las tecnologías de la información y la comunicación, así como la valoración del uso de datos almacenados, procesados o transferidos vinculados a estas tecnologías que afecten los intereses relacionados a la identidad de las personas.
Art 4.-	Acceso indebido a sistemas informáticos	En relación con el acceso indebido o no autorizado, será sancionado con prisión de uno a cuatro años
Art 5.-	Acceso indebido a los programas o datos informáticos.	Hace referencia al acceso de datos con la apropiación o cometer otros delitos, la sanción es equivalente de dos a cuatro años de prisión.
Art 6.-	Interferencia del sistema informático	Se enfoca de manera agravada en la interferencia o alteración en los programas o sistemas informáticos destinados a la prestación de servicios financieros, con una sanción de prisión de tres a seis años.
Art 9.-	Violación de la seguridad del sistema	Cuando este se encuentra restringido y será sancionado con prisión de tres a seis años. No aplica cuando es utilizado para realizar pruebas técnicas o auditorías de procesos o programas.

Fuente: Elaboración propia

Tabla 2 “Ley especial contra los delitos informáticos y conexos”

Capitulo II. De los delitos informáticos		
Art 10.-	Estafa informática	Al manipular o interferir en el ingreso de datos falsos en un sistema, realizando alguna operación informática y se obtenga un beneficio patrimonial para sí o un tercero, se sancionará de dos a cinco años de prisión.
Art 11.-	Fraude informático	Cuando se añadan instrucciones falsas o fraudulentas, en los sistemas de información que permitan obtener provecho para sí, puede ser sancionado con tres a seis años de prisión.
Art. 12.-	Espionaje informático	La obtención de datos con información reservada o confidencial en los sistemas de información es sancionada con prisión de cinco a ocho años.
Art. 13.-	Hurto por medios informáticos.	Se establece la apropiación de bienes tangibles o intangibles, con el fin de obtener beneficios económicos, será sancionado con prisión de dos a cinco años.
Capitulo III. Delitos informáticos relacionados con el contenido de los datos.		
Art. 15.-	Manipulación de registros	Puede desarrollarse para instituciones públicas o privadas, alterando, ocultando en los componentes de los sistemas de información, será sancionado con cinco a ocho años de prisión, también puede ser agravado y si se favorece a la comisión de otro delito puede ser superior la sanción.
Art. 22.-	Hurto de identidad	La suplantación o apropiación de una persona natural o jurídica mediante las TIC, será sancionado con prisión de tres a cinco años. Al obtener beneficios económicos sobre los datos personales, confidenciales o sensibles se establece una sanción con prisión de cinco a ocho años.
Art 24.-	Utilización de datos personales	Al hacer uso de datos personales a través de las TIC, violando confidencialidad y seguridad de datos perjudicando a un tercero, será sancionado con prisión de cuatro a seis años.
Art 25.-	Obtención y transferencia de información de carácter confidencial.	Realizar estas acciones mediante el uso de información que vulnere datos informáticos, es sancionado con prisión de cinco a ocho años.

Fuente: Elaboración propia

1.2.11.2 Ley reguladora del ejercicio de la contaduría.

Esta ley tiene por objeto regular el ejercicio de la profesión de la Contaduría Pública, la función de la Auditoría y los derechos y obligaciones de las personas naturales o jurídicas que las ejerzan. Según esta ley, los contadores públicos intervendrán de forma obligada realizando la compulsión de libros y documentos en la dilucidación de asientos contables, relacionadas con toda clase de juicios, a petición del juez de determinada causa o partes en conflicto. (Art. 17).

Tabla 3: “Ley reguladora del ejercicio de la contaduría pública”

Título II. Responsabilidades de los contadores público		
Art. 17.-	Atribuciones del Contador Público	El auditor puede ejecutar autenticación de libros y documentos en la aclaración de situaciones contables, relacionada con toda clase de discernimiento ya sea a petición de un juez o a solicitud de partes interesadas.

Fuente: Elaboración propia

1.2.11.3 Ley de bancos

Tiene por finalidad regular la intermediación financiera y otras operaciones realizadas por las instituciones bancarias, con el objetivo que estas instituciones le brinden a la población un servicio transparente y más confiable que contribuya al desarrollo del país. Se encuentran los servicios financieros que efectúen los bancos, así como procesos de regularización, reestructuración, intervención y liquidación que se puedan presentar, entre otros.

Tabla 4: “Ley de bancos”

Título III. Capítulo I. Operaciones en general		
Art. 51.-	Tipos de operaciones	Se detallan una lista de operaciones ya sean depósitos a la vista, plazo o ahorro, captaciones de fondos, aceptación de documentos que representan obligaciones de pago, entre otras operaciones.

Fuente: Elaboración propia

1.2.11.4 Código penal.

Dicho código tiene el objeto de orientar nuestra normativa penal dentro de una concepción garantista, de alta efectividad para restringir la violencia social y con una amplia proyección de función punitiva no selectiva, resulta conveniente que se emita un nuevo código penal, que, sin apartarse de nuestros patrones culturales, se constituya en un instrumento moderno, dinámico y eficaz para combatir la delincuencia. En esta ley se regula el delito de estafa: Art. 215 “Para la fijación de la sanción, el juez tomará en cuenta la cuantía del perjuicio, la habilidad o astucia con que el agente hubiere procedido y si este hubiere recaído en persona que por su falta de cultura o preparación fuere fácilmente engañarle”.

Tabla 5: “Código penal”

Capitulo III. De las Defraudaciones		
Art. 215.-	Estafa	Se declara delito de estafa el beneficio injusto en daños a terceros mediante engaños de buena fe, los cuales serán sancionado de dos a cinco años de prisión.

Fuente: Elaboración Propia

CAPÍTULO II: METODOLOGÍA DE LA INVESTIGACIÓN

2.1 Enfoque y tipo de investigación

Basados en la problemática planteada, esta investigación es de naturaleza cualitativa. Con el objeto de estudiar desde las causales del problema, su sistema de relaciones y su estructura dinámica hasta las propuestas de soluciones desde la perspectiva de los auditores forenses involucrados en casos de fraude financiero a través del robo de identidad, para ello, se diseñó un marco teórico que permite conocer las generalidades del fraude financiero y el robo de identidad, sus antecedentes, el impacto que estos han tenido en la sociedad salvadoreña al día de hoy y la normativa técnica y legal pertinente, así como también el rol del auditor forense y el perfil que este debe manejar en el ámbito. Además, para sustentar nuestra postura con miras al objetivo de este trabajo, llevamos a cabo una entrevista a un profesional ejerciente que ha tenido alguna experiencia en estos casos.

2.1.1 Tipo de estudio

El tipo de estudio que se realizó es el hipotético-deductivo, el cual procede de una verdad general hasta llegar al conocimiento de verdades particulares o específicas. Se utilizó este método porque se parte de las generalidades del robo de identidad para descubrir las causales del delito y asimismo proponer una serie de técnicas que el auditor forense podrá aplicar en determinados casos. Estas se han puesto a prueba con un ejemplo práctico.

2.2 Técnicas e instrumentos utilizados en la investigación

2.2.1 Técnicas

- **Sistematización bibliográfica**, Se efectuaron consultas a diferentes materiales bibliográficos de carácter normativo y legal
- **Entrevista**, se obtuvo información de manera directa a través del diálogo y preguntas claves.

2.2.2 Instrumentos

- **Ficha bibliográfica**, se recopila la información extraída de fuentes bibliográficas, necesarias para la investigación.
- **Guía de preguntas para entrevista**, selección de preguntas claves a un profesional para el análisis y obtención directa de la información.

2.3 Sujetos y objeto de estudio

Los profesionales ejercientes de la auditoría hacia dónde se orienta la investigación deben poseer características muy destacadas.

El escepticismo profesional es un elemento crucial en las decisiones del auditor, desde la planeación y ejecución del encargo (incluida la determinación de los riesgos) hasta la decisión sobre el tipo de opinión que emitirá. El escepticismo profesional es aplicado por los auditores al mantener una actitud de cuestionamiento acerca de las aserciones de la gerencia sobre sus informes financieros. Esta actitud lo mantiene alerta ante inconsistencias, omisiones o errores,

y le permite a través de un pensamiento crítico, tomar decisiones que tienden a minimizar los riesgos en la actuación profesional.

En cuanto a su formación como persona el auditor forense debe ser objetivo, independiente, justo, honesto, inteligente, astuto, sagaz, planificador, prudente, precavido. Sobre la base de su experiencia y conocimiento el auditor forense debe ser intuitivo, un sospechado permanente de todo y de todos, capaz de identificar oportunamente cualquier síntoma de fraude, su trabajo debe ser guiado siempre por el escepticismo profesional.

2.4 Unidades de análisis, población y muestra

El análisis se realizó con la colaboración de los profesionales ejercientes.

2.5 Variables e indicadores

2.5.1 Determinación de variables

Variable independiente: Proponer una serie de técnicas especializadas y un adecuado programa de auditoría forense para aplicarlas.

Indicadores:

- Documentología
- Grafología
- Técnicas de entrevista/interrogatorio
- Informática forense

Variable dependiente: Capacidad del auditor forense para detectar fraudes por robo de identidad en el sistema bancario salvadoreño.

Indicadores:

- Conocimientos generales de los principales tipos de robo de identidad y las subcategorías de estos.
- Dominio de la normativa técnica y legal aplicable al robo de identidad financiero.
- Elaboración de programas eficaces para la recolección de evidencia en este tipo de delitos.
- Informes concluyentes con resultados que sirvan como instrumento para procesos judiciales.

2.6 Operacionalización de variables

Tabla 6: “Operacionalización de variables”

Formulación del problema	Objetivo General	Hipótesis del trabajo	Elementos de la hipótesis	Variable	Indicadores	Instrumentos
¿En qué medida mejorará la capacidad del auditor forense para detectar fraudes por robo de identidad en el sistema bancario salvadoreño al proponer una serie de técnicas especializadas y un adecuado programa de auditoría forense para aplicarlas?	Fortalecer la capacidad profesional que requieren los auditores forenses en la aplicación de técnicas especializadas para detectar, mitigar y prevenir los casos de fraudes basados en el robo de identidad dentro del sistema bancario salvadoreño.	El adecuado conocimiento, dominio y aplicación de técnicas especializadas por parte del auditor forense, fortalece su capacidad para detectar de fraudes de robo de identidad en el sistema bancario salvadoreño	Conocimientos generales de los principales tipos de robo de identidad y las subcategorías de estos	Variable independiente: Brindar una serie de técnicas especializadas y un adecuado programa de auditoría forense para aplicarlas.	Aplicación de las siguientes técnicas en una auditoría forense: <ul style="list-style-type: none"> ● Documentología ● Grafología ● Técnicas de entrevista/interrogatorio Informática forense	Ficha bibliográfica, donde se recopila la información fundamental para la investigación Guía de preguntas claves que funcionaran ante la entrevista
			Documentología, grafología, técnicas de entrevista/interrogatorio, informática forense			Variable dependiente: Capacidad del auditor forense para detectar fraudes por robo de identidad en el sistema bancario salvadoreño.
			Mejoras en la identificación de los riesgos de incorrección material orientados al fraude			
			Obtención de evidencia de auditoría suficiente y adecuada Informes concluyentes con resultados que sirvan como instrumento para procesos judiciales			

Fuente: Elaboración propia

2.8 Diagnóstico de la investigación.

A partir del presente estudio cualitativo se identificó la dimensión del inadecuado conocimiento y dominio, de la normativa legal y técnica por parte del auditor forense, los cuales afectan la capacidad en detectar fraudes de robo de identidad, dado que un mínimo de auditores la ha ejercido. A continuación, se presentan las diferentes causas a la problemática:

- Ausencia de recursos de conocimientos fiables. Las expectativas de la información que requieren los profesionales ejercientes son elevadas, los sitios web que proporcionan este tipo de información más complementaria, no son de fácil acceso y muchos de estos no son constantemente de fuentes confiables.
- Los auditores en su gran mayoría no han tenido experiencia alguna realizando trabajos en el ámbito de auditoría forense, lo que viene a dificultar la elaboración de programas efectivos para detectar los puntos clave de la auditoría y por consiguiente su informe concluyente. Por ello, es necesaria una constante capacitación sobre temas de fraude por robo de identidad en todas sus formas, y, además, una guía de realización de programas de auditoría para este tipo de casos que sea funcional para la obtención de evidencia y hallazgos que sean de relevancia para la investigación del delito.
- Dado que la auditoría forense representa un estudio más útil e integral como herramienta especializada para detectar y prevenir delitos financieros, los cuales son vulnerables en relación a los recursos de las organizaciones (factor humano), donde se aprovechan de las debilidades del control interno, el profesional ejerciente no se encuentra en su mayoría con una capacidad para

brindar una asesoría a estos temas a las entidades lo cual vuelve necesario implementar y fortalecer estos contenidos.

Dentro de las disposiciones identificadas para contribuir al aprendizaje de la auditoría forense y su relación con el fraude financiero a través de robo de identidad está implementar las técnicas como la documentología, la informática forense y la entrevista interrogatorio principalmente, para que estas le permitan:

- Conocer la información general de la empresa
- Identificar debilidades en la aplicación del control interno
- Diseñar un programa de auditoría que le ayude a obtener evidencia

El diseño de programas para probar casos de robo de identidad es importantísimo, ya que brinda una guía en cuanto a procedimientos necesarios para probar y evidenciar la ocurrencia de algún ilícito.

Según lo conversado en la entrevista hecha al profesional ejerciente con respecto a la temática planteada se estableció lo siguiente:

- El profesional ejerciente reconoce que el robo de identidad es un riesgo real en la banca electrónica del Sistema Bancario Salvadoreño, el cual presenta sus fallas, y que el auditor forense, con las herramientas y técnicas indicadas, juega un rol importante para la prevención y detección de fraudes a través de estos medios, siendo este un apoyo en la resolución de casos judiciales

CAPÍTULO III: CASO PRÁCTICO

3.1 PLANEACIÓN DE LA AUDITORÍA FORENSE

3.1.1 Introducción

El fraude es una de las principales preocupaciones de una entidad, los porcentajes de pérdidas que las entidades tienen por esta causa son un ejemplo importante para combatirla. La actividad especializada en la prevención y detección del fraude encamina a buscar alternativas como la Auditoría Forense, que se ha convertido en una alternativa para combatir el fraude, participando en investigaciones de ilícitos emitiendo opiniones de valor técnico, que le permiten a la justicia actuar con mayor certeza.

La Auditoría forense es una herramienta para la lucha contra el fraude y la corrupción, para lo cual es indispensable que los niveles máximos de autoridad estén convencidos y comprometidos con las entidades para emprender acciones firmes y definitivas contra estos delitos. La buena seguridad en una empresa depende del manejo eficaz de los recursos tanto financieros, económicos, tecnológicos y humanos para poder controlar de mejor manera el riesgo de fraude, de esta forma las actividades están orientadas a lograr objetivos establecidos por la alta dirección.

En términos generales este documento incluye información general de la entidad bancaria, así como un estudio y evaluación del control interno que permita identificar debilidades en la implementación de dicho control que puedan inducir a cometer fraude. Se incluye el diseño del programa de auditoría forense para la obtención de evidencia.

3.1.2 Objetivos

Objetivo general

- Realizar una auditoría forense a la entidad “BANCO DE DESARROLLO CENTROAMERICANO SOCIEDAD ANONIMA”. Para obtener evidencia suficiente y adecuada que nos permita identificar posibles delitos en la investigación de fraude financiero a través de robo de identidad a los clientes del banco y dar nuestra opinión.

Objetivos específicos

- Verificar el cumplimiento de la normativa legal vigente en El Salvador y aplicable a la entidad.
- Realizar procedimientos de auditoría forense que permitan recolectar evidencia suficiente y adecuada
- Emitir un informe de Auditoría Forense que contenga nuestra opinión sobre el caso investigado en la entidad

3.1.3 Alcance

Nuestros servicios profesionales se desarrollan primordialmente sobre la base de las disposiciones técnicas de la Norma Internacional de Encargos de Aseguramiento, a fin de cumplir con los objetivos del trabajo. La investigación comprenderá el año 2020 y el primer trimestre de 2021

3.1.4 Riesgos

- Que la entidad bancaria no aplique procedimientos de debida diligencia y debida diligencia intensificada.
- Que la data de la bitácora de transacciones electrónicas se encuentre manipulada.
- Que no existan evidencias de los movimientos del personal captados a través de cámaras al interior de la institución.
- Que el personal del área auditada no colabore para la recolección de información relevante para el caso.
- Accesos no autorizados, ya sean realizado por piratas informáticos (hackers) o por empleados del banco (insiders)

3.1.5 Información de la entidad

Banco de Desarrollo Centroamericano, S.A. es una institución financiera que nace en 2012 con sucursales en toda la región Centroamericana incluido El Salvador.

Misión: Somos el banco de los centroamericanos que, a través de servicios financieros y atención personalizada, impulsa los grandes comienzos y contribuye al desarrollo de nuestro país.

Visión: Ser un banco enfocado en personas y empresas, que supere los mil millones de dólares en activos en el 2025.

Los valores de BANDECA son los elementos fundamentales para la generación y mantenimiento de nuestra cultura corporativa. Todos los miembros de la familia BANDECA conocen y viven los valores en su comportamiento, actitudes, y en cada contacto que establecen con nuestros clientes internos, externos y proveedores. Creemos firmemente que la generación

de una cultura de servicio inicia en casa, donde la comunicación organizacional, capacitación y formación constante son parte de nuestro compromiso con nuestros colaboradores. Con estas bases establecidas, buscamos reafirmar el espíritu y deseo por servir e innovar en la banca centroamericana.

3.1.6 Áreas de la entidad:

Área de créditos: Esta área está designada para ofrecer varios tipos de créditos a personas o empresas con el propósito de apoyar a los clientes en sus proyectos personales.

Área de ventas: Esta área se encarga de mostrar los productos que ofrece el banco a los clientes y que se gestione la vinculación del cliente en el sistema bancario.

Área de negocios: Esta área es la que a través de personal capacitado le da continuidad a cada cliente, da soporte técnico, ayuda a ampliar los servicios ofrecidos y atiende cualquier consulta para mejorar la satisfacción de cada persona y empresa.

3.1.7 Calidad en que actúa el profesional ejerciente

El auditor forense se encargará de utilizar sus habilidades y conocimientos en el diseño e implementación de programas de auditoría que ayuden a identificar posibles delitos en la investigación de fraude financiero a través de robo de identidad a los clientes del Banco de Desarrollo Centroamericano (BANDECA).

3.1.8 Sede

Banco de Desarrollo Centroamericano (BANDECA), Agencia San Benito. Bulevar del Hipódromo 665, San Salvador. (El nombre de la entidad es un supuesto, utilizado con fines didácticos).

3.1.9 Definición y tipificación del hecho (tipo de fraude)

En relación con la exposición del riesgo de fraude, se encuentra catalogado en el ciberdelincuencia el cual es definido como una actividad delictiva que afecta o abusa las tecnologías de información, dentro de esta categoría están los accesos no autorizados, donde se encuentra el robo de identidad.

Figura 2: “Exposición al riesgo de fraude, FRAUD TREE”

C i b e r c r i m e n	Piratería	Reproducción o utilización de propiedad intelectual
		Distribución de propiedad intelectual
	Acceso no Autorizado	Espionaje
		Sistemas de Información
		Passwords comprometidos
		Robo de Identidad
		Robo de Información
		Uso dispositivo electrónicos
	Vandalismo	Destrucción de información
		Saboteo sistemas de información
		Interrupción del servicio
		Suplantación del sistema de información o web
		Instalación malware

Fuente: (Cruz, 2021)

3.1.10 Causa

Se recibe la denuncia de cliente en agencia, por posible fraude efectuado en el trámite del crédito móvil 777000024397 y en los retiros de las tarjetas de crédito MasterCard 5369580000683783 y Visa débito 4550005050147086 a nombre de Susana Torio, la cual asegura no utilizar estos productos y solicita una investigación por lo que se procede a verificar si existe el posible incumplimiento en los controles y políticas establecidas por el Banco.

3.1.11 Afectado / ofendido / víctima

Los productos y cuentas para verificar están a nombre de la cliente Susana Torio.

3.1.12 Presunto perpetrador / imputado / acusado

El ejecutivo de negocios Elvis Nieto, ha realizado las evaluaciones de crédito a nombre de la cliente según los registros del sistema MIQ C.

3.1.13 Donde inicia el proceso

Con la denuncia del cliente del banco Susana Torio sobre transacciones que desconoce haber realizado

3.1.14 Donde finaliza

Con el informe de auditoría forense con el cual se tomará la decisión de proceder a realizar la demanda ante las instancias correspondientes de las personas involucradas en el delito cometido.

3.1.15 Flujograma del proceso

Figura 3: “Flujograma del proceso”



Fuente: Elaboración propia

3.2 Antecedentes del caso

Susana Torio es cliente del Banco de Desarrollo Centroamericano (BANDECA). Desde hace varios años, ha solicitado diversos productos y servicios que ofrece dicho banco, siendo su ejecutivo de negocio el señor Elvis Nieto.

El día 15 de agosto de 2020 según el sistema Inbase, la cliente Susana Torio solicitó el usuario de Banca Online, creándose el usuario 090909091 según los registros del archivo maestro de usuarios de la aplicación de internet banking. En esta misma fecha se registra que se efectuó el cambio de contraseña.

El día 5 de septiembre de 2020 se registra el ingreso a la plataforma de banca online el usuario 090909091 asociado a la cliente Susana Torio según bitácora de transacciones y se registra trámite de crédito móvil 777000024397 por un monto de \$4,245.

El desembolso del crédito móvil se realizó a la cuenta de ahorros N.º 026530356758 a nombre de la cliente Susana Torio.

Posterior al desembolso del crédito móvil 777000024397 tramitado por el usuario de banca online 090909091 asociado a la cliente Susana Torio según registros de la bitácora de transacciones electrónicas se efectuaron traslados y pagos de tarjetas de crédito y débito, estas transacciones se realizaron desde la IP 166.852.432.762 asignada al ejecutivo de negocios Elvis Nieto de agencia San Benito.

El día 14 de enero de 2021 se recibió reclamo de la cliente Susana Torio, quien solicitó se investigue un crédito digital realizado en fecha 5 de septiembre de 2020, por un monto de \$4,245.00 el cual no ha solicitado además de los retiros efectuados en las tarjetas de crédito MasterCard 5369580000683783 y Visa débito 4550005050147086, dado que no los ha efectuado. Adicionalmente la cliente manifiesta que su cuenta de ahorro N.º 026530356758 registra abonos y retiros que ella no reconoce.

El día 16 de febrero de 2021 se consultó al sistema IPS, observando que la cliente Susana Torio, registra el teléfono 61349687, el cual difiere con el número que registra la cliente en el “Formulario de Conocimiento del Cliente” del 30/09/2019 y en la solicitud de crédito 5246876 de fecha 5/09/2020, el cual es el 77459472.

3.3 Normativa técnica para la ejecución de la auditoría forense

La finalidad de esta Norma Internacional de Encargos de Aseguramiento (NIEA) es establecer los principios básicos y los procedimientos esenciales, así como proporcionar orientación para la realización, por parte de los profesionales de la contabilidad en ejercicio (denominados “profesionales ejercientes” a efectos de esta NIEA) de encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica, cubiertos por las Normas Internacionales de Auditoría (NIA).

NIEA 3000 (Revisada) Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica, marco internacional de encargos de aseguramiento y las modificaciones de concordancia de otras NIEA.

Esta Norma comprende los trabajos para atestiguar con seguridad razonable y los trabajos para atestiguar con seguridad limitada. El profesional se apoyará especialmente en los apartados:

- Escepticismo y juicio profesionales.
- Planificación y realización del encargo.
- Obtención de evidencia.
- Descripción de los criterios aplicables.
- Formación de la conclusión de aseguramiento.
- Preparación del informe de aseguramiento.
- Documentación.

Normas Internacionales de Auditoría (NIA): emitidas por la Federación Internacional de Contadores (IFAC) a través de la Junta Internacional de Normas de Auditoría y Aseguramiento (IAASB), son un conjunto único de estándares que se aplican a las auditorías para todas las organizaciones, como componente básico para la arquitectura financiera mundial las cuales son indispensables para cualquier auditor independiente.

Dichos estándares ayudan a crear un lenguaje de auditoría común para fortalecer a todas las organizaciones centrado en promover la calidad de la auditoría y las habilidades de los auditores para trabajar en diferentes tipos de entidades: cotizadas y privadas, grandes y pequeñas.

Tabla 8: “Aplicación de Normas Internacionales de Auditoría”

Norma Internacional de Auditoría	Alcance
NIA 240: Responsabilidades del Auditor con respecto al fraude.	La obtención de una seguridad razonable de que los estados financieros considerados en su conjunto están libres de incorrecciones materiales debidas a fraude o error. Debido a las limitaciones inherentes a una auditoría, existe un riesgo inevitable de que puedan no detectarse algunas incorrecciones materiales.
NIA 260: Comunicación con los responsables del gobierno de la entidad	Comunicar claramente a los responsables del gobierno de la entidad, sus responsabilidades en relación con la auditoría y una descripción general del alcance y momento de realización de la auditoría, así como la obtención de información relevante de parte de ellos.
NIA 265: Comunicación de las deficiencias en el control interno a los responsables del gobierno y a la gerencia de la entidad.	En el desarrollo de las pruebas de análisis a los estados financieros por parte del auditor, éste debe informar por escrito sobre las deficiencias encontradas durante el ejercicio de su revisión, a los encargados del gobierno corporativo y administración de la entidad, incluyendo una explicación de los efectos, para que se tomen las medidas correctivas oportunamente

Fuente: Elaboración propia

Tabla 9: “Aplicación de Normas Internacionales de Auditoría”

NIA 315: Identificación y evaluación de los riesgos de error material mediante el conocimiento de la entidad y de su entorno.	El personal auditor debe tener una comprensión de la entidad incluido su ambiente de control interno para identificar y evaluar los riesgos significativos en los estados contables debido a fraudes o errores y que sea apto para ejecutar los procedimientos de auditoría conveniente
NIA 450: Evaluación de los errores identificados durante la realización de la auditoría.	El auditor debe evaluar el efecto de las representaciones erróneas, incluyendo las no corregidas, identificadas durante el análisis de los estados financieros, para determinar si los estados financieros están libres de errores de importancia relativa.
NIA 501: Evidencia de auditoría – Consideraciones específicas para determinadas áreas	Esta norma debe involucrar también los procedimientos que el personal auditor debe llevar a cabo para el conocimiento de litigios que involucren al ente y que pueda repercutir en los estados financieros.
NIA 520: Procedimientos analíticos	El contenido de esta norma obedece a la revisión de las etapas de los planteamientos a utilizar, la recopilación de diferentes elementos de pruebas sustantivas y a una revisión global, provee diferentes pruebas analíticas que dan confianza en su alcance y factores asociados a partidas inusuales para la obtención de evidencias.
NIA 530: Muestreo de auditoría.	La norma establece que utilizar un muestreo estadístico o no es una decisión del auditor, por lo cual allí se diseñan muestreos de población, tamaños de la muestra, selección de la muestra, proyección de los errores y la evaluación del resultado.

Fuente: Elaboración propia

3.4 Estudio y evaluación del control interno

Las entidades bancarias siguen un modelo de gestión y control de riesgos basado en tres líneas de defensa. Las funciones de negocio o actividades que toman o generan exposición a un riesgo constituyen la primera línea de defensa frente al mismo. La asunción o generación de riesgos en la primera línea de defensa debe ajustarse al apetito y los límites definidos. Para atender su función, la primera línea de defensa debe disponer de los medios para identificar, medir, tratar y reportar los riesgos asumidos.

La segunda línea de defensa está constituida por la función de control y supervisión de los riesgos y por la función de cumplimiento. Esta segunda línea vela por el control efectivo de los riesgos y asegura que los mismos se gestionan de acuerdo con el nivel de apetito de riesgo definido.

La Auditoría interna, como tercera línea de defensa y en su labor de última capa de control, evalúa periódicamente que las políticas, métodos y procedimientos son adecuados y comprueba su efectiva implantación.

La función de control de riesgos, la función de cumplimiento y la función de auditoría interna cuentan con el nivel de separación e independencia suficiente, entre sí y respecto de aquellas otras a las que controlan o supervisan, para el desempeño de sus funciones y tienen acceso al consejo de administración y/o sus comisiones a través de sus máximos responsables.

Figura 4: “Líneas de defensa del sistema bancario”



Fuente: Santander. (s.f.). *Gestión de Riesgos*. DDMerc.

Para tener un conocimiento general se realizó un cuestionario de control interno y demás procedimientos para identificar la validez y claridad de la documentación obtenida.

3.5 Evaluación de control interno: Área de negocios

Objetivos:

- Evaluar las actividades de control interno del área de negocios
- Identificar las actividades con debilidades de control interno

Tabla 10: “Cuestionario de control interno”

No	Pregunta	SI	NO	Hecho por	Observación
ENTORNO DE CONTROL					
1	En el área se demuestra el compromiso por los valores éticos y la integridad en su desempeño	X		V.Y.C.G.	
2	Tiene la entidad bancaria políticas para el otorgamiento de créditos debidamente establecidas que cubran aspectos como: <ul style="list-style-type: none"> • El establecimiento de límites en la cantidad autorizada a aprobar sobre un crédito • El requerimiento de la aprobación por parte de junta directiva en aquellos casos que sobrepasen los límites establecidos para el otorgamiento de créditos • El establecimiento de guías y límites para los tipos de préstamos a ofrecer • El establecimiento de políticas para el otorgamiento de préstamos a empleados, miembros de comités y gerencia 	X			
3	La gerencia se involucra en el monitoreo y evaluación de las actividades del departamento de Negocio	X			
EVALUACIÓN DE RIESGOS					
4	Existen requisitos mínimos sobre la información requerida a los solicitantes de créditos y se especifican estos para cada tipo de préstamo	X			

5	Se realiza una investigación de crédito para todas las solicitudes de préstamos y se documenta mediante la obtención del historial crediticio y el análisis de la capacidad de pago	X			
6	los ejecutivos de negocio atienden a los mismos clientes que han solicitado antes algunos productos con ellos		X		No existe política para que un ejecutivo de negocio atienda a los mismos clientes
7	Se asigna a cada ejecutivo de negocio un cliente diferente independientemente que ya haya solicitado productos con el	X			
8	Personal que no sea del departamento de crédito puede acceder a los archivos de registros de usuarios de banca en línea	X			
9	Se tienen claves de acceso diferentes para cada empleado autorizado de acceder a archivos relacionados a transacciones de banca en línea.	X			
10	Se revisan las cuentas de empleados del banco periódicamente por un auditor o comité de supervisión		X		
11	La máquina que grava las tarjetas está bajo un control estricto para que solo el personal autorizado pueda tener acceso	X			
ACTIVIDADES DE CONTROL					
12	La Gerencia ejerce un rol activo en la revisión de las políticas para el otorgamiento de créditos para asegurarse de que son consistentes con las condiciones del mercado y cumplen con los objetivos del banco	X			
13	Todos los préstamos y líneas de créditos ya sea que se originen o se renueven son aprobados por el comité de crédito en fiel cumplimiento con las normas y políticas para el otorgamiento de créditos	X			
14	¿Se requiere una solicitud de crédito para todos los préstamos?	X			
15	Con relación a los préstamos con garantía				

16	<p>hipotecaria:</p> <ul style="list-style-type: none"> • Se verifica y documenta la titularidad de la garantía ofrecida antes de la aprobación del préstamo • Se requiere evidencia del pago de seguros en los casos de propiedades que así lo requieren antes de la aprobación del préstamo <p>Se utiliza una lista de cotejo y se revisa la inclusión en el expediente del préstamo de toda la documentación requerida</p>	X X X			
17	Existe un contrato de autorización para la creación de banca en línea de los clientes	X			
18	<p>Existe solicitud en la banca en línea para el otorgamiento de los siguientes productos</p> <ul style="list-style-type: none"> • Tarjeta de crédito • Crédito móvil • Cuenta de ahorro 	X X X			
INFORMACION Y COMUNICACIÓN					
19	La gerencia recibe y analiza informes sobre la actividad en el departamento de créditos (otorgados, renovados y denegados)	X			
20	<p>Con relación a la revisión interna de los créditos otorgados:</p> <ul style="list-style-type: none"> • El personal a cargo de esta función es independiente a las funciones de origen, desembolso, contabilidad y cobro • El personal que desempeña esta función identifica y evalúa problemas existentes a tiempo a manera que se establezcan medidas correctivas • Los resultados de estas revisiones internas son informados a junta directiva y/o comité de crédito 	X X X			
21	Hay una segregación adecuada de tareas				

22	entre las siguientes funciones: <ul style="list-style-type: none"> ● Aprobación de préstamos ● Desembolso de préstamos ● Control de pagares ● Registro de las transacciones de los préstamos 	X X X X X			
23	La documentación de los préstamos preparada por los ejecutivos de créditos es inspeccionada por una persona independiente para asegurarse que esté completa y correcta antes de la aprobación del crédito	X			
	Se tiene control que la información se genera de manera oportuna				
ACTIVIDADES DE MONITOREO					
24	tiene el personal capacitaciones constantes sobre la concientización de cometer delitos de fraudes	X			
25	Cuando hay fallas en los sistemas, son comunicadas con claridad al encargado del área	X			
26	Se realizan evaluaciones continuas de los procesos de crédito que se generan en el área de negocios	X			

Fuente: Elaboración propia

3.6 Controles internos

Se cumplirá con todos los procedimientos de control interno establecidos por el banco para garantizar una correcta contabilización de las transacciones y su adecuado reflejo en la información financiera publicada por el banco.

Al preparar la información financiera las funciones del banco responsables de cada actividad, proceso y subproceso deberán certificar que han cumplido con los controles establecidos y que la información suministrada es correcta. El Comité de Auditoría supervisará

el proceso de presentación de la información financiera, la eficacia del control interno y la auditoría interna. El Comité de Riesgos (denominado en la Corporación la Comisión de supervisión de riesgos, regulación y cumplimiento) supervisará los sistemas de gestión de riesgos. El Código General de Conducta atribuye a la dirección y al resto de empleados, en el nivel que les corresponda, responsabilidades en relación con las obligaciones anteriores

3.7 Riesgos

- Que el banco no aplique procedimientos de debida diligencia y debida diligencia intensificada.
- Que la data de la bitácora de transacciones electrónicas se encuentre manipulada.
- Que no existan evidencias de los movimientos del personal captados a través de cámaras al interior de la institución.
- Que el personal del área auditada no colabore para la recolección de información relevante para el caso.
- Accesos no autorizados, ya sean realizado por piratas informáticos (hackers) o por empleados del banco (insiders).

3.8 Limitaciones

Dificultad para entrevistar a personas que serían clave dentro de la investigación.

3.9 Planilla de Decisiones Preliminares

Figura 5: “Planilla de decisiones preliminares”

PLANILLA DE DECISIONES PRELIMINARES BANDECA, S. A.													
COMPONENTE	INDICIOS DEL FRAUDE OBTENIDOS	FACTORES DE RIESGO ESPECIFICO	EVALUACION DE RIESGO									PROCEDIMIENTOS DE AUDITORIA QUE CORRESPONDEN A FACTORES DE RIESGO	CONSIDERACIONES SOBRE ALCANCE
			INHERENTE			CONTROL			DETECCION				
			A	M	B	A	M	B	A	M	B		
Manejo de cuentas financieras existentes o creación de nuevas cuentas suplantando la identidad de la víctima	Transacciones no efectuadas por el cliente.	Riesgo de Seguridad											
		Diseño de Sistema: Aplicación y Mantenimiento			X			X	X				Verificar el inventario de IP versus las IP registrada en la bitácora de transacciones electrónicas
Venta de la información personal de la víctima, para ser utilizada para falsificación de documentos, o aprovecharse de las vulnerabilidades de los seguros	Alertas de inicio de sesión no reconocidas en internet banking	Riesgo Operacional											
		Accesos no autorizados - Falta de controles de accesos	X				X				X	Analizar la descripción del puesto de cada ejecutivo de negocio	Conocer los procedimientos que tiene permitido realizar al atender a los clientes
Uso de la cuenta bancaria de la víctima para operaciones de blanqueo de dinero.	Número de teléfono móvil no reportado por la cliente, difiere del formulario del conocimiento del cliente	Fraudes de empleados	X				X			X		Aplicación de procedimientos analíticos relacionados con cuentas de ingresos (cuentas de ahorro y/o cuentas corrientes) de los posibles	Identificar transacciones inusuales que pueden indicar riesgos de incorrección material debida a fraude
		El cliente no cumple las pautas de seguridad		X			X			X		Revisar según huellas de auditoría el historial de actualizaciones de datos que se realizaron para cada usuario de la Banca Online de cada uno de los clientes que han	Verificar desde qué medio proceden y si estas actualizaciones han sido solicitadas realmente por los clientes.
		El cliente niega haber realizado una transacción			X			X	X			Cruzar los documentos de identificación e información personal versus los datos registrados en el sistema, de los clientes que presentan reclamos	Verificar la debida confidencialidad de la información y que estos no presenten alteraciones
		Riesgo Legal											
		Protección a la Privacidad			X			X	X			Revisar en el archivo INBASE (bitácora de transacciones electrónicas) los registros de transacciones realizadas por los clientes que han presentado reclamo al banco al comparar la base de datos de casos SIGMA (bitácora de denuncias de clientes)	verificar si procede o no el reclamo y si existen casos vinculados o de naturaleza similar al reclamo presentado por los clientes
Realizar transferencias o compras con cuentas vigentes	Posible cambios en la calificación crediticia	Riesgo reputacional											
		migración de fondos a otras entidades		X				X		X		Entrevista a los clientes	Conocer el procedimiento que realizó en la captación de datos personales por parte de BANDECA

Fuente: Elaboración propia.

3.10 Programas de Auditoría

Tabla 11: “Programas de auditoría”.

PROCEDIMIENTOS DE AUDITORÍA FORENSE PARA LA DETECCIÓN DE FRAUDE FINANCIERO ENFOCADO EN EL ROBO DE IDENTIDAD EN EL ÁMBITO BANCARIO SALVADOREÑO	
Objetivo y Alcance:	Evaluar y probar el grado de la calidad que el sistema de control interno posee, para depositar su confianza en la realización de las operaciones vinculadas a los clientes, y verificar si existe violación en las políticas y procedimientos aprobados por BANDECA. La comprensión de la información podrá documentarse a través de un cuestionario de control interno.
Objetivos Específicos:	<p>Los objetivos de la investigación incluyen evaluar las condiciones identificadas y determinar:</p> <ul style="list-style-type: none"> • Los hechos relacionados con el trámite de crédito móvil No. 777000024397 y retiros en efectivo de tarjetas de crédito y débito a nombre de la cliente Susana Torio. • Determinar si existió violación a las políticas y procedimientos aprobados por BANDECA • Determinar si existe evidencia para remitir los casos a las autoridades judiciales
Definiciones relevantes:	<p>Base de datos: Programa capaz de almacenar gran cantidad de datos, relacionados y estructurados, que pueden ser consultados rápidamente de acuerdo con las características selectivas que se deseen</p> <p>Casos Sigma: Base de datos donde se detalla el registro de los reclamos de los clientes perfilado por naturaleza, fecha, NIU, documentos de identidad y tipo de productos.</p> <p>INBASE: Software de gestión de procesos y contenido empresarial.</p> <p>IP: conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo o que corresponde al nivel de red de modelo TCP/IP.</p>

<i>No.</i>	<i>Procedimiento</i>	<i>Hecho por:</i>	<i>Referencia Pts.</i>
1	Realizar indagaciones ante la dirección del fraude, incluidas la naturaleza, la extensión y la frecuencia, para determinar cuáles son las áreas en las que se debe enfocar una mejora.		
2	Solicitar manual de políticas y procedimientos de otorgamiento de los productos financieros ofrecidos por BANDECA, para verificar si cumplen con los requerimientos de una estructura organizacional acorde a los productos, servicios, operaciones, perfil de riesgos y modelo de negocio, de tal forma que		

<i>No.</i>	<i>Procedimiento</i>	<i>Hecho por:</i>	<i>Referencia Pts.</i>
	delimite claramente las facultades asociadas a la seguridad de la información y la ciberseguridad.		
3	Analizar la descripción del puesto de cada ejecutivo de negocio para conocer los procedimientos que tiene permitido realizar al atender a los clientes		
4	Solicitar los expedientes de préstamos de los clientes que han hecho reclamo al banco por transacciones no efectuadas por ellos, cruzando los documentos de identificación e información personal versus los datos registrados en el sistema, para verificar la debida confidencialidad de la información y que estos no presenten alteraciones		
5	Revisar en el archivo INBASE (bitácora de transacciones electrónicas) los registros de transacciones realizadas por los clientes que han presentado reclamo al banco al comparar la base de datos de casos SIGMA (bitácora de denuncias de clientes), para verificar si procede o no el reclamo y si existen casos vinculados o de naturaleza similar al reclamo presentado por los clientes		
6	Solicitar el inventario de las IP de la agencia San Benito para verificar los números de los equipos de cada ejecutivo de ventas y atención al cliente de BANDECA de acuerdo con las IP registradas en la bitácora de transacciones electrónicas, con el fin de identificar si alguno de ellos ha tenido participación en las transacciones de los clientes que han presentado reclamos.		
7	Diagnosticar y conocer las conexiones entrantes en el equipo, verificar e identificar la dirección IP de un sitio web, para detectar la actividad de troyanos, spam y otras intrusiones en las PC, también indispensable para poder diagnosticar cualquier conflicto de redes.		
8	Realizar gestión de vulnerabilidades identificando y evaluando las medidas de seguridad en la infraestructura tecnológica, mediante la ejecución de pruebas de penetración o intrusión y de escaneos de vulnerabilidades. Se deberán remediar todas las brechas de seguridad no solo las clasificadas como críticas y de alto riesgo.		
9	Solicitar la base de datos de los ejecutivos de negocios de la Agencia San Benito, según la cartera de clientes apertura da por los productos ofrecidos por BANDECA, para verificar si los clientes que han presentado reclamos de la misma naturaleza pertenecen a un solo ejecutivo de negocios		
10	Evaluar si se identifican transacciones inusuales o inesperadas que pueden indicar riesgos de incorrección material debida a fraude, mediante la aplicación de procedimientos analíticos relacionados con cuentas de ingresos (cuentas de ahorro y/o cuentas corrientes) de los posibles implicados al caso.		
11	Revisar según huellas de auditoría el historial de actualizaciones de datos que se realizaron para cada usuario de la Banca Online de cada uno de los clientes que		

<i>No.</i>	<i>Procedimiento</i>	<i>Hecho por:</i>	<i>Referencia Pts.</i>
	han presentado reclamos para verificar desde qué medio proceden y si estas actualizaciones han sido solicitadas realmente por los clientes.		
12	Solicitar la base de tarjetas de crédito activas de los clientes que han presentado reclamos, para verificar los movimientos y traslados de saldos según el número de la tarjeta y la IP de la cual se ha producido la transacción electrónica.		
13	Solicitar los videos de vigilancia de la agencia San Benito en las fechas en que los clientes que han reclamado se han presentado a la sucursal para solicitar la creación de su usuario de banca en línea y así monitorear si ha habido irregularidades en el proceso		
14	Revisar base de datos del área de call center de BANDECA para determinar el registro de llamadas realizadas y recibidas por los clientes que han realizado reclamo al banco, así como fechas y horas en que se realizaron y Solicitar las grabaciones de las llamadas		
15	Revisar los correos electrónicos del área de call center del banco, recibidos y enviados que tengan relación con los clientes que han presentado reclamo al banco		
16	Entrevistar a uno de los clientes que ha sido afectado para saber el procedimiento que realizó en la captación de datos personales por parte de BANDECA		
17	Entrevistar al ejecutivo de ventas involucrado en el caso para analizar sus interacciones con los clientes afectados		
	Conclusión		
16	Concluya sobre el trabajo realizado		

Observaciones:

Preparado:	Nelson Gabriel Sánchez Puentes	Fecha:	Firma
Supervisado:	Vilma Yesenia Cáceres Guevara	Fecha:	Firma
Aprobado:	Rocío Estefany Alvarado Maravilla	Fecha:	Firma

Fuente: Elaboración propia

3.11 Análisis FODA de la entidad en El Salvador

Tabla 12: “Análisis FODA de la entidad en El Salvador”

Factores de éxito		Factores críticos	
Fortalezas	Oportunidades	Debilidades	Amenazas
Diversidad de productos financieros	Mayor inversión en sucursales a nivel nacional	Tasas de interés poco competitivas	Devaluación constante de la moneda
Infraestructura moderna y adecuada para las actividades de la entidad	Publicidad a través de diferentes medios de comunicación	Nivel de quejas alto por parte de los clientes	Aumento del mercado de las criptomonedas
Facilidades para la obtención de créditos	Crecimiento de los saldos en las cuentas corrientes de los clientes	Poca supervisión de los ejecutivos de venta y créditos	Alto riesgo de estafas a través de la banca electrónica
Compromiso por los valores éticos y la integridad en su desempeño	Aumento de las pequeñas y medianas entidades	Limitada red de cajeros a nivel nacional	Aumentan los requerimientos y regulaciones para la banca
Se cuenta con un equipo tecnológico avanzado para el manejo de datos de los clientes			
Todo el personal cuenta con capacitaciones periódicas en cada área			

Fuente: Elaboración propia

3.12 Personal clave

Área de Negocios / Ejecutivo de Ventas Internas: Es el encargado de ofertar las ventas de los productos que ofrece el banco a los clientes y que se gestione la vinculación del cliente en el sistema bancario.

3.13 Personal designado

Socio encargado: Rocío Estefany Alvarado Maravilla

Auditor forense: Vilma Yesenia Cáceres Guevara

Supervisor: Nelson Gabriel Sánchez Puentes

3.14 Desarrollo del programa de auditoria forense



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 1
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Realizar un cuestionario de control interno	Revisado por	V.C.
Periodo:	del 1 de enero de 2020 al 30 de junio de 2021		

Procedimiento: Realizar indagaciones ante la dirección del área sobre la valoración del riesgo mediante un Cuestionario de Control interno, que pueda incluir incorrecciones materiales debido al fraude, incluidas la naturaleza, la extensión y la frecuencia, para determinar cuáles son las áreas en las que se debe enfocar una mejora.

Se extendió un cuestionario a la gerencia de negocios de BANDECA con el objetivo de determinar deficiencias en el control interno de área. Los resultados fueron los siguientes:

CUESTIONARIO DE CONTROL INTERNO				
No.	Pregunta	Sí	No	Observación
ENTORNO DE CONTROL				
1	En el área se demuestra el compromiso por los valores éticos y la integridad en su desempeño	X		
2	Tiene la entidad bancaria políticas para el otorgamiento de créditos debidamente establecidas que cubran aspectos como:			
	El establecimiento de límites en la cantidad autorizada a aprobar sobre un crédito	X		
	El requerimiento de la aprobación por parte de junta directiva en aquellos casos que sobrepasen los límites establecidos para el otorgamiento de créditos	X		
	El establecimiento de guías y límites para los tipos de préstamos a ofrecer	X		
	El establecimiento de políticas para el otorgamiento de préstamos a empleados, miembros de comités y gerencia	X		
3	La gerencia se involucra en el monitoreo y evaluación de las actividades del departamento de Negocio			
EVALUACIÓN DE RIESGOS				
4	Existen requisitos mínimos sobre la información requerida a los solicitantes de créditos y se especifican estos para cada tipo de préstamo	X		
5	Se realiza una investigación de crédito para todas las solicitudes de préstamos y se documenta mediante la obtención del historial crediticio y el análisis de la capacidad de pago	X		
6	Los ejecutivos de negocio atienden a los mismos clientes que han solicitado antes algunos productos con ellos		X	

7	Se asigna a cada ejecutivo de negocio un cliente diferente independientemente que ya haya solicitado productos con el	X		
8	Personal que no sea del departamento de crédito puede acceder a los archivos de registros de usuarios de banca en línea	X		
9	Se tienen claves de acceso diferentes para cada empleado autorizado de acceder a archivos relacionados a transacciones de banca en línea.	X		
10	Se revisan las cuentas de empleados del banco periódicamente por un auditor o comité de supervisión		X	
11	La máquina que grava las tarjetas está bajo un control estricto para que solo el personal autorizado pueda tener acceso	X		
ACTIVIDADES DE CONTROL				
12	La Gerencia ejerce un rol activo en la revisión de las políticas para el otorgamiento de créditos para asegurarse de que son consistentes con las condiciones del mercado y cumplen con los objetivos del banco	X		
13	Todos los préstamos y líneas de créditos ya sea que se originen o se renueven son aprobados por el comité de crédito en fiel cumplimiento con las normas y políticas para el otorgamiento de créditos	X		
14	¿Se requiere una solicitud de crédito para todos los préstamos?			
15	Con relación a los préstamos con garantía hipotecaria:			
	Se verifica y documenta la titularidad de la garantía ofrecida antes de la aprobación del préstamo	X		
	Se requiere evidencia del pago de seguros en los casos de propiedades que así lo requieren antes de la aprobación del préstamo	X		
16	Se utiliza una lista de cotejo y se revisa la inclusión en el expediente del préstamo de toda la documentación requerida	X		
17	Existe un contrato de autorización para la creación de banca en línea de los clientes	X		
18	Existe solicitud en la banca en línea para el otorgamiento de los siguientes productos:			
	Tarjeta de crédito	X		
	Crédito móvil	X		
	Cuenta de ahorro			
INFORMACIÓN Y COMUNICACIÓN				
19	La gerencia recibe y analiza informes sobre la actividad en el departamento de créditos (otorgados, renovados y denegados)	X		
20	Con relación a la revisión interna de los créditos otorgados:			
	El personal a cargo de esta función es independiente a las funciones de origen, desembolso, contabilidad y cobro	X		
	El personal que desempeña esta función identifica y evalúa problemas existentes a tiempo a manera que se establezcan medidas correctivas	X		
	Los resultados de estas revisiones internas son informados a junta directiva y/o comité de crédito	X		
21	Hay una segregación adecuada de tareas entre las siguientes funciones:			
	Aprobación de préstamos	X		
	Desembolso de préstamos	X		
	Control de pagarés	X		
	Registro de las transacciones de los préstamos	X		

	La documentación de los préstamos preparada por los ejecutivos de créditos es inspeccionada por una persona independiente para asegurarse que esté completa y correcta antes de la aprobación del crédito	X		
23	Se tiene control que la información se genera de manera oportuna	X		
ACTIVIDADES DE MONITOREO				
24	Tiene el personal capacitaciones constantes sobre la concientización de cometer delitos de fraudes	X		
25	Cuando hay fallas en los sistemas, son comunicadas con claridad al encargado del área	X		
26	Se realizan evaluaciones continuas de los procesos de crédito que se generan en el área de negocios	X		

Conclusión: En general el área de negocios está fortalecida en sus procesos de capacitación a los empleados y en atención a los clientes, sin embargo, con este cuestionario encontramos dos deficiencias que pueden ser claves. Primero, que un mismo empleado puede atender a un mismo cliente en todas las variedades de servicios que estos ofrecen, lo que puede generar un vínculo extraprofesional entre el empleado y el cliente que esté fuera del control de la agencia y segundo, que no existe una supervisión constante de las cuentas del ejecutivo de negocios en BANDECA.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 2
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Políticas relacionadas a la banca en línea	Revisado por	V.C.
Periodo:	del 1 de enero de 2020 al 30 de junio de 2021		

Procedimiento: Solicitar manual de políticas y procedimientos de otorgamiento de los productos financieros ofrecidos por BANDECA, para verificar si cumplen con los requerimientos de una estructura organizacional acorde a los productos, servicios, operaciones, perfil de riesgos y modelo de negocio, de tal forma que delimite claramente las facultades asociadas a la seguridad de la información y la ciberseguridad.

Se verificaron todas las políticas de BANDECA relacionadas al otorgamiento de sus servicios, en las que resaltamos las siguientes, las cuales tienen que ver con el uso de su plataforma en línea (banca electrónica) para realizar operaciones por parte de los clientes:

“EL CLIENTE” acepta expresamente que “EL BANCO” le presta los SERVICIOS DE BANCA ELECTRÓNICA, mediante el uso de equipos y sistemas automatizados y de conformidad a lo establecido en el artículo cincuenta y seis literal “1” de la Ley de Bancos, cuyas regulaciones contractuales se entienden incorporadas y adicionadas a los Contratos de Servicios de Banca Electrónica, Depósito en Cuenta Corriente, Ahorros, Préstamos y Tarjetas de Crédito y débito, y otros celebrados entre “EL CLIENTE” y “EL BANCO”, bajo los términos, condiciones y obligaciones siguientes:

1. “EL BANCO” concede a “EL CLIENTE” el servicio de acceso a las diferentes operaciones bancarias que éste ofrece, u ofreciere en el futuro, contratadas con aquél, por medio de la utilización de equipos, dispositivos y sistemas automatizados que “EL BANCO” proporcione al Cliente, por medio de los cuales éste puede realizar todas las operaciones bancarias que “EL BANCO” ponga a su disposición.
2. Las operaciones bancarias que “EL CLIENTE” podrá realizar incluyen, pero no están limitadas a, consultar saldos de sus cuentas corrientes de ahorro, préstamos, depósitos a plazo, tarjetas de crédito y tarjetas de débito emitidas por “EL BANCO”, solicitud de compra de chequeras, reserva de cheques, tele pago; transferir fondos entre cuentas propias, realizar pagos a préstamos, tarjetas de créditos, servicios públicos, colegiaturas, y cualquier otro pago periódico o eventual que “EL CLIENTE” requiera realizar con terceros que tengan cuenta con “EL BANCO”; retiros de dinero en efectivo, compras y pagos en diferentes establecimientos de comercio afiliados a Visa Internacional; cambio de identificación electrónica secreta; y cualquier otro servicio que en el futuro “EL BANCO” ofrezca a sus clientes.
3. Los equipos y sistemas automatizados a que se hace referencia corresponden, y no están limitados, a la Red de Cajeros Automáticos BANDECA y otras redes locales e internacionales de Cajeros Automáticos afiliados a Visa Internacional y PLUS, Puntos de Venta, Internet, telefonía fija o móvil, además de otros equipos y sistemas automatizados que en el futuro “EL BANCO” ofrezca a sus clientes.
4. “EL BANCO” se obliga a guardar confidencialidad en la asignación y manejo de la identificación electrónica secreta y personal de “EL CLIENTE”.
5. “EL CLIENTE” podrá acceder a los servicios que aquí se detallan como servicios de Banca Electrónica a través de mecanismos de identificación electrónica que “EL BANCO” le proporcione, tales como claves de números, lectores de huellas digitales, retina, y cualquier otro sistema o mecanismo de seguridad

biométrica o de otro tipo que en un futuro "EL BANCO" disponga para la prestación de sus servicios. Es entendido que: a) "EL CLIENTE" tendrá única y absoluta responsabilidad por la custodia, confidencialidad, por el uso o mal uso que dé a la identificación electrónica secreta, o por el retiro indebido de fondos, y cualquier otro acto ilícito o punible, a partir de la fecha del respectivo contrato; b) toda información obtenida, y toda operación realizada utilizando la identificación electrónica secreta, se entenderá que ha sido realizada por "EL CLIENTE" o autorizada por él mismo; c) "EL CLIENTE" exonera de toda responsabilidad a "EL BANCO" por cualquier perjuicio que se ocasione por el uso indebido de la identificación electrónica secreta, entendiéndose que "EL CLIENTE" asume cualquier consecuencia derivada de ella; d) "EL CLIENTE" exonera a "EL BANCO" de cualquier suspensión temporal de los servicios por caídas de líneas de comunicación en los sistemas, así como por la falta de acceso al servicio por falla del equipo o del servicio del proveedor, si lo hubiera, y cualquier suspensión de los servicios por causas no imputables a "EL BANCO"; e) "EL BANCO" proporcionará a "EL CLIENTE" una identificación electrónica secreta para el acceso a todos los servicios ofrecidos mediante el respectivo contrato; f) "EL CLIENTE" conoce y comprende, por explicación dada por "EL BANCO", los efectos e implicaciones del respectivo contrato, del uso de los sistemas y equipos automatizados, el valor probatorio de esta identificación electrónica secreta, de los estados de cuenta, reportes de saldos y movimientos, y de la sustitución de la firma por claves secretas, u otro medio de identificación electrónica.

6. Es entendido que por el carácter electrónico de este servicio, esta identificación electrónica secreta es personal, intransferible e intransmisible, y sustituye la firma autógrafa de "EL CLIENTE"; por lo tanto, toda la información obtenida y toda operación realizada utilizando dicha identificación electrónica secreta, se entenderá que ha sido firmada, consentida y autorizada por "EL CLIENTE", siendo la constancia emitida por los registros electrónicos de "EL BANCO" prueba absoluta y suficiente para demostrar y comprobar la existencia de toda consulta, transacción y operación bancaria derivada del respectivo contrato, facultando a "EL BANCO" a cargar o abonar en cualquiera de las cuentas que "EL CLIENTE" posea con "EL BANCO" o cualquiera de sus filiales, el valor de esos comprobantes.

7. "EL CLIENTE" se obliga a: a) cambiar su clave o identificación electrónica secreta la primera vez que accede al sistema, y cambiarla periódicamente a fin de mantener la confidencialidad del servicio, y evitar el uso indebido de la misma; b) que las transacciones que realice en uso del presente servicio no violen leyes o disposiciones legales, obligándose especialmente a brindar la información exigida por la Ley contra el Lavado de Dinero y de Activos; c) notificar por escrito dentro de los treinta días de haberse recibido los estados de cuenta o reportes de saldos y movimientos, de las operaciones bancarias realizadas en uso de los diferentes servicios, las inconsistencias u observaciones de tales operaciones; si transcurre dicho plazo sin que "EL CLIENTE" hubiese efectuado tales observaciones, dichos estados de cuenta o reportes de saldos y movimientos se tendrán como válidos.

8. "EL CLIENTE" queda obligado de aportar a "EL BANCO" las pruebas de toda operación anulada, defraudada o duplicada en el uso de los diferentes servicios. Al efecto, "EL BANCO" tomará en consideración para el análisis de dichas operaciones, los comprobantes que "EL CLIENTE" presente relativos a las transacciones reclamadas.

9. En caso de pérdida de la tarjeta de débito, de la identificación electrónica secreta, o en caso de robo o uso ilícito de las mismas, "EL CLIENTE" deberá reportar por escrito inmediatamente ocurrido el suceso a "EL BANCO" o deberá llamar por teléfono inmediatamente al Centro de Llamadas de "EL BANCO" (Call Center).

10. "EL CLIENTE" manifiesta que entiende que "EL BANCO" tiene definidas condiciones y limitaciones para el funcionamiento de los diferentes servicios; por lo tanto, las opciones que "EL BANCO" designe para cada uno de los canales de acceso a los diferentes servicios, podrán restringirse o ampliarse; de igual manera podrán incluirse nuevas opciones que "EL BANCO" asigne a cada uno de ellos.

11. "EL CLIENTE" autoriza a "EL BANCO" para cargar o abonar del saldo de cualquiera de las cuentas que posea en "EL BANCO", o en cualquiera de sus filiales, todo gasto, comisión, cargo, recargo, calor de transacción o cualquiera otra erogación publicada conforme a la ley que implique el uso de los presentes servicios, las cuales podrán ser modificadas en cualquier tiempo mediante su previa publicación legal por "EL BANCO".

12. A partir de la firma del respectivo contrato queda a opción de "EL CLIENTE" gozar automáticamente de los beneficios del "Programa de Protección contra Robo y Uso Ilícito de Tarjetas de Débito" mediante un pago periódico, conforme se detalla en Adendum respectivo al contrato respectivo, cuyo valor se especifica en la tabla de comisiones publicada por "EL BANCO" mensualmente y depende del monto asegurado, mismo que "EL CLIENTE" ha seleccionado en la solicitud de Servicios de Banca Electrónica,

en el espacio destinado para tal fin, en el entendido que: a) "EL CLIENTE" debe reportar cualquier reclamo conforme a la Cláusula Diez del presente documento; b) el programa no cubre retiros de efectivo en cajeros automáticos; c) La responsabilidad de "EL BANCO" se limita a responder por transacciones ilícitas hasta por el monto máximo de cobertura contratada; d) "EL BANCO" se reserva el derecho de realizar las gestiones necesarias a efecto de calificar la ilicitud de las operaciones, y solicitar certificación de Aviso a la Policía para deducir la responsabilidad del caso; e) el programa no tendrá aplicación en caso de comprobarse responsabilidad de "EL CLIENTE", o en caso que la cuenta principal asociada a la tarjeta de débito se encuentre sobregirada al momento de realizar el reclamo; f) "EL BANCO" podrá poner término al presente programa en cualquier tiempo, notificándolo a "EL CLIENTE" mediante publicación en un periódico de circulación nacional; g) El plazo del "Programa de Protección contra Robo y Uso Ilícito de la Tarjeta de Débito" será de 15 años a partir de la fecha de la firma de la solicitud; h) "EL BANCO", en los casos que proceda, al realizar el reintegro a la cuenta de "EL CLIENTE" o emitir el cheque de gerencia para pago del seguro, realizará el cobro del deducible correspondiente al seguro contratado, el cual se encuentra definido de igual forma en el Adendum respectivo al contrato respectivo.

13. En caso que "EL CLIENTE" quiera renunciar a los beneficios del "Programa de Protección contra Robo y Uso Ilícito de Tarjetas de Débito", deberá llenar y firmar el formulario que "EL BANCO" posee para ese fin, en cualquiera de sus Agencias y Minibancos, y a partir de ese momento, "EL BANCO" no tendrá ninguna responsabilidad en caso de robo, pérdida, o uso ilícito, de la tarjeta de débito.

14. "EL CLIENTE" expresamente autoriza a "EL BANCO", para que pueda asociar con la firma del respectivo contrato cualquiera de sus cuentas abiertas en "EL BANCO", o en cualquiera de sus filiales, de forma indistinta a los servicios objeto del respectivo contrato. La asociación podrá ser rechazada por "EL CLIENTE" siempre y cuando, este presente una carta donde manifieste expresamente su deseo de no asociar una o varias cuentas.

15. "EL CLIENTE" reconoce y acepta que los presentes servicios corresponden a servicios tecnológicos electrónicos, por lo que "EL CLIENTE" se responsabiliza de su código personal y del buen cuidado de la(s) tarjeta(s) plásticas con banda magnética o chip, proporcionada(s) para tal fin.

16. "EL CLIENTE" declara expresamente que "EL BANCO" le ha leído y explicado en forma clara, veraz, oportuna y satisfactoria, las obligaciones y condiciones que aquí se señalan y por ello las acepta.

Conclusión: Todas las políticas anteriormente leídas cumplen con los requisitos de ciberseguridad que el Sistema Financiero espera por parte de BANDECA para resguardar la información del cliente y contribuya a la prevención del fraude electrónico. Encontramos dentro de estas una de las claves para la investigación; el banco debe garantizar la confidencialidad en la asignación y manejo de la identificación secreta y personal del cliente.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoría:	Forense	REF.	PT 3
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Analizar la descripción del puesto del ejecutivo	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		
Procedimiento:	Analizar la descripción del puesto de cada ejecutivo de negocio para conocer los procedimientos que tiene permitido realizar al atender a los clientes.		

Se solicitó la descripción del puesto de ejecutivo de negocios para conocer las atribuciones, funciones y objetivos que estos tienen, se describe a continuación:

DESCRIPCIÓN DEL PUESTO: EJECUTIVO DE NEGOCIOS:

Objetivo General del Puesto:

Promover a clientes actuales y potenciales productos activos, pasivos y de seguros, con el fin de alcanzar las metas establecidas en el presupuesto para contribuir al crecimiento de la rentabilidad y participación de mercado y lograr la satisfacción del cliente.

Retos del Puesto:

- ❖ Administrar la percepción del cliente sobre la excelencia operativa y servicio al cliente en BANDECA.
- ❖ Cumplir integralmente las metas de ventas de productos establecidas.
- ❖ Realizar "buena venta": Que cada relación creada deje una buena experiencia de compra al cliente.
- ❖ Resolver reclamos y quejas con la mejor solución de cara al cliente.

Principales Funciones:

- ❖ Vender la propuesta de servicio correspondiente al perfil del cliente asignado (Personal, Especial) que pertenezca a su micro-mercado, que él visite y/o contacte telefónicamente.
- ❖ Mantener una tubería de potenciales nuevos clientes para atraerlos mediante la proposición que corresponda hacia BANDECA.
- ❖ Realizar venta cruzada utilizando productos activos, seguros, cuentas corrientes y de ahorros.
- ❖ Ejecutar “servicio al cliente” de acuerdo a la filosofía Institucional, ejecutar los protocolos de atención, y procesar quejas y reclamos relacionados.
- ❖ Asegurar que la información que entregan los clientes es veraz y hacer el análisis preliminar de cumplimiento de perfiles autorizados por la institución.
- ❖ Obtención de Información para evaluación crediticia de clientes dentro del buró externo para originación de créditos de banca de personas.
- ❖ Procesar en el sistema las solicitudes de créditos, vigilar que se cumpla adecuadamente los manuales de procesos, políticas y normas de créditos de BANDECA.

Conclusión: En la descripción del puesto se tienen contempladas las funciones del ejecutivo de manera adecuada a los productos que la institución ofrece, pero esta descripción no detalla los límites de los empleados de acuerdo a las prohibiciones en las políticas de servicios de la institución, por lo



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria: Forense **REF. PT 4**
Cliente: BANDECA S.A. **Preparado por N.S.**
Cedula: Expediente de préstamos de clientes **Revisado por V.C.**
Periodo: Del 1 de enero de 2020 al 30 de junio de 2021

Procedimiento: Solicitar los expedientes de préstamos de los clientes que han hecho reclamo al banco por transacciones no efectuadas por ellos, cruzando los documentos de identificación e información personal versus los datos registrados en el sistema, para verificar la debida confidencialidad de la información y que estos no presenten alteraciones

Se solicitó al banco el expediente de los préstamos de todos los clientes que ha presentado reclamos por irregularidades en sus cuentas para verificar si la información que ellos proporcionaron en sus solicitudes ha sido modificada sin su consentimiento, el detalle se presenta a continuación con el siguiente cuadro:

Nombre del cliente	Documento de Identidad (DUI)	Segmento de Crédito	Referencia del Crédito	Forma de Crédito	Monto Contratado	Tasa de Interés Nominal Anual	Tasa de Interés Mensual	Fecha de Otorgamiento	Fecha de Vencimiento	Periodicidad de Pago	Cuota de Préstamo	Numero de Cuotas	Seguros y Otros Cargos en la Cuota	Membresía anual o comisión por	Teléfono de referencia
Andrés Trozado	03648273-5	1	2145622	1	\$ 5,000.00	15.23%	1.27%	15/03/2020	14/03/2024	5	\$ 139.74	48	\$ 50.00	No	7527-4563
Ana Tomía	01123627-4	2	2145645	1	\$ 5,500.00	15.23%	1.27%	07/01/2019	06/01/2023	5	\$ 97.82	48	\$ 50.00	No	6126-2783
Ramona Ponte Alegre	02638363-3	2	2145652	1	\$ 6,000.00	15.23%	1.27%	13/01/2019	12/01/2024	5	\$ 143.46	60	\$ 50.00	No	7532-4692
Matías Queroso	01343647-6	4	2145659	3	\$ 7,500.00	18.64%	1.95%	15/01/2019	14/01/2024	5	\$ 193.07	60	\$ 50.00	No	6539-5038
Cristiano Rolando	02113617-4	1	2145666	1	\$ 3,600.00	15.23%	1.27%	05/02/2019	04/02/2023	5	\$ 100.61	48	\$ 50.00	No	7112-0284
Armando Puentes	02343647-6	4	2145673	3	\$ 7,200.00	18.64%	1.95%	10/02/2019	09/02/2024	5	\$ 185.35	60	\$ 50.00	No	6825-2964
Aitor Tilla	04451256-9	1	2145680	1	\$ 2,000.00	15.23%	1.27%	11/02/2019	10/02/2022	5	\$ 69.56	36	\$ 50.00	No	7710-3719
Lola Mento	03123627-4	2	2145687	1	\$ 6,000.00	15.23%	1.27%	03/03/2019	02/03/2023	5	\$ 167.68	48	\$ 50.00	No	7037-2947
Zoyla Vaca	02613256-5	2	2145694	1	\$ 3,000.00	15.23%	1.27%	05/04/2019	04/04/2023	5	\$ 89.84	48	\$ 50.00	No	7402-2947
Susana Torio	04113617-4	1	2145701	1	\$ 5,000.00	15.23%	1.27%	30/04/2019	29/04/2023	5	\$ 139.74	48	\$ 50.00	No	7594-3894
Elena Nito	05113617-4	1	2145708	1	\$ 4,500.00	15.23%	1.27%	08/05/2019	07/05/2023	5	\$ 125.76	48	\$ 50.00	No	6639-4086
Antonio Calvo	05133637-1	3	2145715	1	\$ 600.00	12.02%	1.00%	14/05/2019	13/05/2020	5	\$ 53.31	12	\$ -	Si	6199-4096
Inés Pinilla	05353657-8	5	2145722	3	\$ 8,500.00	18.64%	1.95%	21/05/2019	19/05/2026	5	\$ 181.85	84	\$ 50.00	No	7836-0373
Armando Paredes	06133637-1	3	2145729	1	\$ 1,500.00	12.02%	1.00%	17/06/2019	16/06/2020	5	\$ 133.29	12	\$ -	Si	6294-8362
Julio Feo	06113617-4	1	2145736	1	\$ 2,800.00	15.23%	1.27%	22/06/2019	21/06/2023	5	\$ 78.25	48	\$ 50.00	No	7120-4090
Miguel Marco Gol	02638363-2	2	2145743	1	\$ 2,500.00	15.23%	1.27%	16/08/2019	15/08/2023	5	\$ 69.87	48	\$ 50.00	No	7991-0983
Helen Chufe	09113617-4	1	2145750	1	\$ 4,400.00	15.23%	1.27%	26/09/2019	25/09/2023	5	\$ 122.97	48	\$ 50.00	No	7772-3090
Armando Bronca	12353657-9	5	2145757	3	\$ 12,500.00	18.64%	1.95%	01/12/2019	28/11/2029	5	\$ 251.41	96	\$ 50.00	No	7913-0936
Flor del Campo	07638363-4	7	2145764	2	\$ 9,100.00	18.64%	1.95%	25/01/2020	24/01/2024	5	\$ 270.37	48	\$ 100.00	No	7103-2098
David Bacán	01123627-4	2	2145771	1	\$ 4,000.00	15.23%	1.27%	31/01/2020	30/01/2024	5	\$ 111.79	48	\$ 50.00	No	7777-3093
Petronilo Prezo	02343647-6	4	2145778	3	\$ 6,000.00	18.64%	1.95%	06/02/2020	04/02/2025	5	\$ 154.46	60	\$ 50.00	No	7209-9053
Elsa Pato	02123627-6	2	2145785	1	\$ 6,000.00	15.23%	1.27%	13/02/2020	11/02/2025	5	\$ 143.46	60	\$ 50.00	No	7121-3987

Conclusión: Considerando el expediente inicial de cada cliente y confrontándolo con el actualizado se logró verificar que la cliente Susana Torio presenta una solicitud de actualización de datos en el que se cambió el número de teléfono asociado a su cuenta, del 7594-3894 al 7727-6853, el cual pertenece al móvil personal de uno de los ejecutivos de BANDECA.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 5
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Bitácora de Transacciones Inusuales	Revisado por	V.C.
Periodo:	DEL 1 DE ENERO DE 2020 AL 30 DE JUNIO DE 2021		

Procedimiento: Revisar en el archivo INBASE (bitácora de transacciones electrónicas) los registros de transacciones realizadas por los clientes que han presentado reclamo al banco al comparar la base de datos de casos SIGMA (bitácora de denuncias de clientes), para verificar si procede o no el reclamo y si existen casos vinculados o de naturaleza similar al reclamo presentado por los clientes.

Se revisó el archivo INBASE (bitácora de transacciones electrónicas) de las cuentas de la cliente Susana Torio y se identificaron los siguientes movimientos desde la banca en línea:

USUARIO	FECHA	HORA	NÚMERO DE TARJETA DE CRÉDITO	CUENTA DE AHORROS ABONADA	MONTO
90909091	15/08/2020	17:29	5369580000683780	26530356758	\$1210.85
90909091	15/08/2020	15:43	5369580000683780	26530356758	\$ 1,000.00
90909091	20/08/2020	11:20	5369580000683780	777000024397	\$400.00
90909091	25/10/2020	14:33	5369580000683780	777000024397	\$584.00
90909091	04/11/2020	18:55	5369580000683780	777000024397	\$ 250.00
90909091	07/12/2020	18:06	5369580000683780	777000024397	\$600.00
90909091	07/01/2021	15:27	5369580000683780	777000024397	\$550.00
90909091	14/01/2021	19:01	5369580000683780	777000024397	\$500.00
90909091	04/02/2021	13:25	4555294627972010	777000024397	\$600.00
90909091	09/02/2021	12:23	4555294627972010	26530356758	\$1,100.00
90909091	15/12/2020	18:18	4555294627972010	26530356758	\$ 350.00
Total, retiros en tarjeta de crédito					\$7144.85

Conclusión: los anteriores movimientos corresponden a traslados de fondos de tarjetas de créditos a cuentas de ahorro de la clienta, estos fueron consultados con Susana Torio y ella los desconoce, afirma que no fueron realizados por su persona. El monto de todas estas transacciones asciende a \$6,334.00, pero ninguno de ellos corresponde a gestiones realizadas por la clienta.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 6
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Verificación de Inventario de IP de Agencia San Benito	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		

Procedimiento: Solicitar el inventario de las IP de la agencia San Benito para verificar los números de los equipos de cada ejecutivo de ventas y atención al cliente de BANDECA de acuerdo con las IP registradas en la bitácora de transacciones electrónicas, con el fin de identificar si alguno de ellos ha tenido participación en las transacciones de los clientes que han presentado reclamos.

Se solicitó el inventario de las IP que se encuentran asignadas en la Agencia San Benito, con el fin de verificar la cantidad de ellas, así como el número registrado según el personal de la Agencia, en especial a los Ejecutivos de Ventas y los que se encuentran en Atención al cliente, se identificó que la IP registrada número 166.852.432.762, se encuentra también en la bitácora de transacciones electrónicas, y en la base de casos sigma, la cual esta asignada al ejecutivo de ventas internas Elvis Nieto, de la Agencia San Benito.

Código	Agencia	Número de IP	Asignada a
PC-546456	San Benito	146.752.432.261	Perla de Oriente
PC-231548	San Benito	166.852.432.762	Elvis Nieto
PC-123147	San Benito	175.313.213.163	Samsung Rodriguez
PC-151547	San Benito	366.944.770.704	Georgia Santos
PC-897984	San Benito	540.219.762.765	Edenilson Wisconsin
PC-4546789	San Benito	948.314.832.917	Liseth Motorola

Conclusión: Todas las políticas anteriormente leídas cumplen con los requisitos de ciberseguridad que el Sistema Financiero espera por parte de BANDECA para resguardar la información del cliente y contribuya a la prevención del fraude electrónico. Encontramos dentro de estas una de las claves para la investigación; el banco debe garantizar la confidencialidad en la asignación y manejo de la identificación secreta y personal del cliente.



Tipo de Auditoria:	Forense	REF.	PT 7
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Verificación de conexiones entrantes	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		
Procedimiento:	Diagnosticar y conocer las conexiones entrantes en el equipo, verificar e identificar la dirección IP de un sitio web, para detectar la actividad de troyanos, spam y otras intrusiones en las PC, también indispensable para poder diagnosticar cualquier conflicto de redes.		

Se hizo el cierre de todos los programas y conexiones a la red, se abrió una ventana con el símbolo del sistema, para eso se escribe en el cuadro de inicio: CMD y se presiona la tecla Enter. En la ventana de la consola de CMD o MSDOS que se abre, ingresa tal como está escrito: NETSTAT- n 10. Lo que se muestra en la pantalla negra de la consola, es una tabla con 4 columnas y diversas filas que contiene la información:

- Proto: Indica el protocolo utilizado para la comunicación por cada una de las conexiones activas (La más importante es la TCP).
- Dirección Local: Indica la dirección origen de la conexión y después el puerto.
- Dirección Remota: Indica la dirección de destino, su IP y el puerto.
- Estado: Indica el estado de la conexión en cada momento

Los estados posibles son:

- LISTENING: El puerto está escuchando en espera de una conexión
- ESTABLISHED: La conexión ha sido establecida
- CLOSE_WAIT: La conexión sigue abierta, pero el otro extremo comunica que no se enviara nada.
- TIME_WAIT: La conexión ha sido cerrada, pero no se elimina de la tabla de conexión, estado pendiente.
- LAST_ACK: La conexión se está cerrando.
- CLOSED: La conexión ha sido cerrada definitivamente

```

Administrador: C:\Windows\system32\cmd.exe - NETSTAT
C:\Users\AYERIM\Desktop>NETSTAT
Conexiones activas
  Proto Dirección local      Dirección remota      Estado
C:\Users\AYERIM\Desktop>NETSTAT
Conexiones activas
  Proto Dirección local      Dirección remota      Estado
  TCP   127.0.0.1:2869       AYERIM-PC:49185      TIME_WAIT
  TCP   190.6.74.39:49184    65.54.161.12:http     TIME_WAIT
  TCP   190.6.74.39:49186    ultraserver2:http     ESTABLISHED
  TCP   190.6.74.39:49187    ultraserver2:http     ESTABLISHED
  TCP   190.6.74.39:49188    ultraserver2:http     ESTABLISHED
  TCP   190.6.74.39:49189    ord08s06-in-f3:https  ESTABLISHED
  TCP   190.6.74.39:49190    ord08s06-in-f3:https  ESTABLISHED
  TCP   190.6.74.39:49191    a72-246-215-139:http  ESTABLISHED
  TCP   190.6.74.39:49192    a72-246-215-139:http  ESTABLISHED
  
```

Conclusión: No se han identificado conexiones de IP inusuales en NETSTAT.



Tipo de Auditoria:	Forense	REF.	PT 8
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Gestión de vulnerabilidades	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		
Procedimiento:	Realizar gestión de vulnerabilidades identificando y evaluando las medidas de seguridad en la infraestructura tecnológica, mediante la ejecución de pruebas de penetración o intrusión y de escaneos de vulnerabilidades. Se deberán remediar todas las brechas de seguridad no solo las clasificadas como críticas y de alto riesgo.		



Este análisis nos servirá para averiguar la magnitud y la gravedad de las consecuencias del riesgo a la que está expuesta nuestra empresa y, de esta forma, gestionarlos adecuadamente. Para ello tendremos que definir un umbral que determine los riesgos asumibles de los que no lo son. En función de la relevancia de los riesgos podremos optar por:

- Evitar el riesgo eliminando su causa, por ejemplo, cuando sea viable optar por no implementar una actividad o proceso que pudiera implicar un riesgo.
- Adoptar medidas que mitiguen el impacto o la probabilidad del riesgo a través de la implementación y monitorización de controles.
- Compartir o transferir el riesgo con terceros a través de seguros, contratos etc.
- Aceptar la existencia del riesgo y monitorizarlo

Conclusión: Las medidas de seguridad en infraestructura tecnológica, ejecutadas mediante pruebas de penetración o intrusión no demuestran ninguna señal de alerta que estén vulnerables o expuestas a un ataque.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria: Forense **REF. PT 9**

Cliente: BANDECA S.A. **Preparado por N.S.**

Cedula: Narrativa de Verificación de Clientes que han presentado reclamos. **Revisado por V.C.**

Periodo: Del 1 de enero de 2020 al 30 de junio de 2021

Procedimiento: Solicitar la base de datos de los ejecutivos de negocios de la Agencia San Benito, según la cartera de clientes apertura da por los productos ofrecidos por BANDECA, para verificar si los clientes que han presentado reclamos de la misma naturaleza pertenecen a un solo ejecutivo de negocios

Se solicitó la base de datos de atención de productos de la Agencia San Benito, por categoría de NIU (Número de Identificación Único de Clientes), fecha, tipo de producto, nombre de cliente, y ejecutivo de negocios, y se cotejó contra la base de casos sigma donde se reporta la naturaleza de reclamos que han presentado los clientes, esta se filtró a nombre del ejecutivo Elvis Nieto, verificando que a parte de la señora Susana Torio, existen dos clientes más que presentan similar caso y fueron vinculados por el mismo ejecutivo Elvis Nieto bajo la IP 166.852.432.762, la cual se encuentra asignada a él.

NIU	Fecha de Vinculación	Nombre del cliente	Documento de Identidad (DUI)	Tipo de Producto	Ejecutivo de Negocios	Agencia	Referencia del Crédito	Forma de Crédito	Monto Contratado	Tasa de Interés Nominal Anual
289704616	13/11/2014	Andrés Trozado	03648273-5	Cuenta de Ahorros	Samsung Rodriguez	San Benito	2145622	1	5000	15,23%
149834127	04/05/2019	Ana Tomía	01123627-4	Credito Movil	Elvis Nieto	San Benito	2145645	1	3500	15,23%
321544746	11/06/2016	Ramona Ponte Alegre	02638363-3	Deposito a Plazo	Perla de Oriente	San Benito	2145652	1	6000	15,23%
159347299	11/01/2015	Matías Queroso	01343647-6	Tarjeta de Credito	Perla de Oriente	San Benito	2145659	3	7500	18,64%
187170064	08/05/2020	Cristiano Rolando	02113617-4	Cuenta de Ahorros	Edenilson Wisconsin	San Benito	2145666	1	3600	15,23%
893120183	11/02/2017	Armando Puentes	02343647-6	Deposito a Plazo	Elvis Nieto	San Benito	2145673	3	7200	18,64%
217833484	24/03/2020	Aitor Tilla	04451256-9	Cuenta Corriente	Elvis Nieto	San Benito	2145680	1	2000	15,23%
478796131	19/06/2020	Lola Mento	03123627-4	Tarjeta de Credito	Liseth Motorola	San Benito	2145687	1	6000	15,23%
423508447	14/08/2020	Zoyla Vaca	02613256-5	Deposito a Plazo	Edenilson Wisconsin	San Benito	2145694	1	3000	15,23%
253320647	17/12/2017	Susana Torio	04113617-4	Credito Movil	Elvis Nieto	San Benito	2145701	1	5000	15,23%
205833847	14/02/2015	Elena Nito	05113617-4	Cuenta de Ahorros	Edenilson Wisconsin	San Benito	2145708	1	4500	15,23%
187112384	07/01/2020	Antonio Calvo	05133637-1	Deposito a Plazo	Georgia Santos	San Benito	2145715	1	600	12,02%
121846103	15/07/2015	Inés Pinilla	05353657-8	Credito Movil	Perla de Oriente	San Benito	2145722	3	8500	18,64%
861177352	30/08/2019	Armando Paredes	06133637-1	Crédito de Consum	Samsung Rodriguez	San Benito	2145729	1	1500	12,02%
154745461	27/11/2016	Julio Feo	06113617-4	Cuenta de Ahorros	Edenilson Wisconsin	San Benito	2145736	1	2800	15,23%
706611681	25/11/2018	Miguel Marco Gol	02638363-2	Tarjeta de Credito	Edenilson Wisconsin	San Benito	2145743	1	2500	15,23%
306481601	09/12/2015	Helen Chufe	09113617-4	Cuenta Corriente	Samsung Rodriguez	San Benito	2145750	1	4400	15,23%
678940694	26/02/2019	Armando Bronca	12353657-9	Crédito de Consum	Elvis Nieto	San Benito	2145757	3	12500	18,64%
121498314	03/08/2020	Flor del Campo	07638363-4	Credito Movil	Edenilson Wisconsin	San Benito	2145764	2	9100	18,64%
589132548	01/07/2017	David Bacán	01123627-4	Tarjeta de Credito	Perla de Oriente	San Benito	2145771	1	4000	15,23%
886465147	19/03/2016	Petronilo Pienzo	02343647-6	Crédito de Consum	Edenilson Wisconsin	San Benito	2145778	3	6000	18,64%
304854878	19/06/2017	Elsa Pato	02123627-6	Crédito de Consum	Elvis Nieto	San Benito	2145785	1	6000	15,23%
165657988	07/10/2014	Ángel de Dios	04638363-7	Crédito de Consum	Liseth Motorola	San Benito	2145792	3	10000	18,64%
561632132	24/06/2020	Alan Brito Delgado	07638363-2	Cuenta de Ahorros	Liseth Motorola	San Benito	2145799	2	10500	18,64%
489481234	17/08/2016	Disney Landia Rodríguez	04638363-2	Cuenta de Ahorros	Edenilson Wisconsin	San Benito	2145806	3	9000	18,64%
453513154	06/11/2015	Zacarías Flores del Campo	03263667-7	Cuenta Corriente	Georgia Santos	San Benito	2145813	2	25000	18,64%
318024849	28/10/2017	Elba Lazo	03133637-1	Crédito de Consum	Edenilson Wisconsin	San Benito	2145820	1	800	12,02%
235478614	23/10/2014	Omar Ciano	04123627-4	Cuenta de Ahorros	Georgia Santos	San Benito	2145827	1	4500	15,23%
314848784	17/09/2019	Igor Dito	04123627-4	Cuenta de Ahorros	Liseth Motorola	San Benito	2145834	1	5000	15,23%
876453653	09/12/2018	Alba Surita	04113617-4	Crédito de Consum	Elvis Nieto	San Benito	2145841	1	3700	15,23%
456456456	06/04/2019	Oscar Acol	04343647-8	Cuenta Corriente	Samsung Rodriguez	San Benito	2145848	3	8700	18,64%
132151654	03/10/2017	Ana Busado de Hesa	05353657-6	Cuenta Corriente	Perla de Oriente	San Benito	2145855	3	7500	18,64%
123132156	28/07/2014	Lucas Carón	05133637-1	Crédito de Consum	Samsung Rodriguez	San Benito	2145862	1	1000	12,02%
012220216	08/11/2015	Alfonso Acosta	06123627-1	Deposito a Plazo	Samsung Rodriguez	San Benito	2145869	1	3000	15,23%

Conclusión: De la base de casos sigma, se encuentran dos clientes más con la misma naturaleza de reclamos y estos se encuentran en la base de datos de la cartera de clientes apertura das por el mismo ejecutivo Elvis Nieto



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 10
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Verificación de Cuentas de Ingresos	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		

Procedimiento: Evaluar si se identifican transacciones inusuales o inesperadas que pueden indicar riesgos de incorrección material debida a fraude, mediante la aplicación de procedimientos analíticos relacionados con cuentas de ingresos (cuentas de ahorro y/o cuentas corrientes) de los posibles implicados al caso.

Se revisó el archivo INTAS (bitácora de transacciones electrónicas, según el usuario de banca online 90909091, asociado al NIU 253320647 de la cliente Susana Torio, la cual registra el ingreso de la Banca Online desde la IP166.852.432.762 asignada al ejecutivo Elvis Nieto de Agencia San Benito y registra trámite de crédito móvil 777000024397 por \$4,145.00. Según las cámaras de Agencia San Benito, a la hora del trámite del crédito no hay presencia de la cliente Susana Torio, y es de mencionar que ella no tiene acceso a dicho equipo, dado que el dueño es el Banco, a continuación, se detalla los registros del trámite de crédito móvil según archivos INTAS (bitácora de transacciones electrónicas).

Usuario de Internet	Fecha	Hora	NIU	Canal	Descripción	Monto	IP donde se realizó la transacción
90909091	15082020	10:01:54	253320647	Login	Login exitoso	0,00	IP166.852.432.762
90909091	15082020	10:02:03	253320647	Consultas	Resumen de cuentas	0,00	IP166.852.432.762
90909091	15082020	10:04:15	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	10:04:49	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	10:15:27	253320647	Logout	Salir	0,00	IP166.852.432.762
90909091	15082020	12:19:35	253320647	Login	Login exitoso	0,00	IP166.852.432.762
90909091	15082020	12:19:44	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	12:27:05	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	13:27:21	253320647	Logout	Salir	0,00	IP166.852.432.762
90909091	15082020	14:45:09	253320647	Login	Login exitoso	0,00	IP166.852.432.762
90909091	15082020	14:45:48	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	14:57:29	253320647	Servicios Bancarios	Crédito móvil desembolsado (exitoso)	4,145,00	IP123.000.000.009

El desembolso del crédito móvil está parametrizado para que se efectúe a una cuenta de la cliente que lo tramita, por lo que el monto neto del crédito móvil 777000024397, por \$4,150.00, se abonó a la cuenta de ahorros 026530356758 a nombre de la cliente Susana Torio. Posteriormente al desembolso, el usuario de Banca Online 90909091, asociado al NIU 253320647 de la cliente Susana Torio, registra ingreso a conexión personal desde la IP166.852.432.762 asignada al ejecutivo Elvis Nieto de Agencia San Benito, y registra que se realizaron traslados y pagos de tarjeta de crédito, según detalle:

Usuario	Fecha	Hora	Cuenta que se abonó con desembolso	Monto	IP donde se realizó la transacción
90909091	15082020	15:18:31	Tarjeta de Crédito 5369580000683783	1,500.00	IP166.852.432.762
90909091	16082020	10:07:25	de la cliente Susana Torio	824.30	IP166.852.432.762
90909091	18082020	12:21:43	Cuenta de ahorros 026530356758 de la cliente Susana Torio	1,500.00	IP166.852.432.762
Total				3,824.30	

Conclusión: Del desembolso por \$4,140.00 quedaron en la cuenta de ahorros 026530356758 de la cliente Susana Torio, un remanente de \$ 315.70 los cuales fueron utilizados por la cliente.



ADVISORS INTERNACIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 11
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Verificación de Procedencia de Casos Sigma.	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		

Procedimiento: Revisar según huellas de auditoría el historial de actualizaciones de datos que se realizaron para cada usuario de la Banca Online de cada uno de los clientes que han presentado reclamos para verificar desde qué medio proceden y si estas actualizaciones han sido solicitadas realmente por los clientes.

Se revisó el historial de actualizaciones de datos que se realizaron para cada usuario de la Banca Online de cada uno de los clientes que han presentado reclamos, estas han sido procedidas de la base de datos de Casos Sigma donde se lleva el registro de reclamos que presentan los clientes, y efectivamente cada uno de los reclamos procede a ser verificado según la naturaleza del caso.

NIU	Caso SIGMA	Nombre del cliente	Documento de Identidad (DUJ)	Tipo de Producto	Ejecutivo de Negocios	Agencia	IP	F
289704616	22453	Andrés Trozado	03648273-5	Crédito de Consumo	Perla de Oriente	San Benito	175.313.213.163	
149834127	22107	Ana Tomía	01123627-4	Cuenta Corriente	Samsung Rodriguez	San Benito	146.752.432.261	
321544746	26809	Ramona Ponte Alegre	02638363-3	Cuenta Corriente	Elvis Nieto	San Benito	540.219.762.765	
159347299	25001	Matías Queroso	01343647-6	Cuenta Corriente	Elvis Nieto	San Benito	366.944.770.704	
187170064	27410	Cristiano Rolando	02113617-4	Credito Movil	Samsung Rodriguez	San Benito	175.313.213.163	
893120183	23364	Armando Puentes	02343647-6	Credito Movil	Liseth Motorola	San Benito	366.944.770.704	
217833484	29217	Aitor Tilla	04451256-9	Deposito a Plazo	Samsung Rodriguez	San Benito	366.944.770.704	
478796131	21639	Lola Mento	03123627-4	Credito Movil	Elvis Nieto	San Benito	540.219.762.765	
423508447	23875	Zoyla Vaca	02613256-5	Deposito a Plazo	Liseth Motorola	San Benito	366.944.770.704	
253320647	26941	Susana Torio	04113617-4	Cuenta Corriente	Elvis Nieto	San Benito	166.852.432.762	
205833847	28683	Elena Nito	05113617-4	Tarjeta de Credito	Elvis Nieto	San Benito	166.852.432.762	
187112384	23424	Antonio Calvo	05133637-1	Cuenta de Ahorros	Edenilson Wisconsin	San Benito	948.314.832.917	
121846103	25488	Inés Pinilla	05353657-8	Cuenta de Ahorros	Samsung Rodriguez	San Benito	166.852.432.762	
861177352	27666	Armando Paredes	06133637-1	Crédito de Consumo	Perla de Oriente	San Benito	146.752.432.261	
154745461	26001	Julio Feo	06113617-4	Tarjeta de Credito	Georgia Santos	San Benito	146.752.432.261	
706611681	29401	Miguel Marco Gol	02638363-2	Cuenta de Ahorros	Elvis Nieto	San Benito	948.314.832.917	
306481601	29016	Helen Chufo	09113617-4	Deposito a Plazo	Elvis Nieto	San Benito	948.314.832.917	
678940694	28865	Armando Bronca	12353657-3	Crédito de Consumo	Elvis Nieto	San Benito	166.852.432.762	
121498314	25779	Flor del Campo	07638363-4	Crédito de Consumo	Perla de Oriente	San Benito	540.219.762.765	
589132548	21662	David Bacán	01123627-4	Cuenta Corriente	Edenilson Wisconsin	San Benito	948.314.832.917	
886465147	28239	Petronilo Pienzo	02343647-6	Cuenta de Ahorros	Perla de Oriente	San Benito	146.752.432.261	
304854878	22563	Elsa Pato	02123627-6	Cuenta Corriente	Elvis Nieto	San Benito	175.313.213.163	
165657988	25026	Ángel de Dios	04638363-7	Cuenta de Ahorros	Liseth Motorola	San Benito	146.752.432.261	
561632132	27445	Alan Brito Delgado	07638363-2	Cuenta de Ahorros	Elvis Nieto	San Benito	175.313.213.163	
489481234	26813	Disney Landia Rodríguez	04638363-2	Credito Movil	Samsung Rodriguez	San Benito	948.314.832.917	
453513154	22168	Zacarías Flores del Campo	03263667-7	Credito Movil	Samsung Rodriguez	San Benito	948.314.832.917	
318024849	24983	Elba Lazo	03133637-1	Tarjeta de Credito	Edenilson Wisconsin	San Benito	166.852.432.762	
235478614	28104	Omar Ciano	04123627-4	Crédito Movil	Elvis Nieto	San Benito	175.313.213.163	
314848784	27619	Igor Dito	04123627-4	Credito Movil	Samsung Rodriguez	San Benito	948.314.832.917	
876453653	26877	Alba Surita	04113617-4	Cuenta de Ahorros	Samsung Rodriguez	San Benito	948.314.832.917	
456456456	28547	Oscar Acol	04343647-8	Crédito de Consumo	Perla de Oriente	San Benito	175.313.213.163	
132151654	23944	Ana Busado de Hesa	05353657-6	Deposito a Plazo	Georgia Santos	San Benito	540.219.762.765	
123132156	22794	Lucas Carón	05133637-1	Cuenta Corriente	Samsung Rodriguez	San Benito	540.219.762.765	
212320315	26410	Marcia Ana	05133637-1	Crédito de Consumo	Edenilson Wisconsin	San Benito	540.219.762.765	

Conclusión: los reclamos presentados por los clientes proceden, para ser verificados según la naturaleza de los casos presentados de cada uno.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoría: Forense
Cliente: BANDECA S.A.
Cedula: Verificación de Base de Tarjetas de Créditos
Periodo: Del 1 de enero de 2020 al 30 de junio de 2021

REF. PT 12
Preparado por N.S.
Revisado por V.C.

Procedimiento: Solicitar la base de tarjetas de crédito activas de los clientes que han presentado reclamos, para verificar los movimientos y traslados de saldos según el número de la tarjeta y la IP de la cual se ha producido la transacción electrónica

Según registros del archivo INTAS (bitácora de transacciones electrónicas) registra que posterior a los traslados de los saldos realizados de las tarjetas de crédito a las cuentas de ahorros de la cliente Susana Torio, se realizaron los pagos y transferencias a varias cuentas entre ellas abonos a tarjetas de crédito a Alan Nieto, padre del ejecutivo de ventas internas Elvis Nieto.

Cuenta de ahorros que recibió abono de la tarjeta de crédito	Monto abonado	Fecha de transacción	Referencia Pagada	Nombre de Cliente de la referencia Pagada	Monto	IP donde se realizó la transacción
26530356758	\$ 1.210,85	15082020	4550005050147080	Tarjeta de débito de la cliente Susana Torio	\$ 32,85	IP166.852.432.762
		15082020	4456005465411567	Tarjeta de crédito de Ever Nieto (padre del ejecutivo Elvis Nieto)	\$ 270,00	IP166.852.432.762
		15082020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 908,00	IP166.852.432.762
Total					\$ 1.210,85	
26530356758	\$ 1.000,00	15082020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 1.000,00	IP166.852.432.762
Total					\$ 1.000,00	
777000024397	\$ 400,00	20082020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 400,00	IP166.852.432.762
Total					\$ 400,00	
777000024397	\$ 584,00	25102020	4550005050147080	Tarjeta de débito de la cliente Susana Torio	\$ 95,00	IP166.852.432.762
		25102020	Retiro Sin Tarjeta	Según video quien retira es ejecutivo Elvis Nieto	\$ 270,00	Mobile Internet Banking
		25102020	Retiro Sin Tarjeta	Según video quien retira es ejecutivo Elvis Nieto	\$ 219,00	Mobile Internet Banking
Total					\$ 584,00	
777000024397	\$ 250,00	4112020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 250,00	IP166.852.432.762
Total					\$ 250,00	
777000024397	\$ 600,00	7122020	Retiro Sin Tarjeta	Según video quien retira es ejecutivo Elvis Nieto	\$ 350,00	Mobile Internet Banking
		6012021	Retiro Sin Tarjeta	Según video quien retira es ejecutivo Elvis Nieto	\$ 250,00	Mobile Internet Banking
		Total				
777000024397	\$ 550,00	7012021	5369580000683783	Tarjeta de crédito de la cliente Susana Torio	\$ 50,00	IP166.852.432.762
		7012021	Retiro Sin Tarjeta	Según video quien retira es ejecutivo Elvis Nieto	\$ 200,00	Mobile Internet Banking
		13012021	Retiro Sin Tarjeta	Según video quien retira es ejecutivo Elvis Nieto	\$ 300,00	Mobile Internet Banking
Total					\$ 550,00	
777000024397	\$ 500,00	14012021	4456005465411567	Tarjeta de crédito de Ever Nieto (padre del ejecutivo Elvis Nieto)	\$ 250,00	IP166.852.432.762
		15012021	26650510887	Cuenta de ahorros de Elvis Nieto	\$ 250,00	IP166.852.432.762
		Total				
777000024397	\$ 600,00	4022021	7771561564397	Préstamo móvil de la cliente Susana Torio	\$ 105,00	IP166.852.432.762
		4022021	5369580000683783	Tarjeta de crédito de la cliente Susana Torio	\$ 108,00	IP166.852.432.762
		5022021	26530356758	Cuenta de ahorros de la cliente Susana Torio	\$ 300,00	Mobile Internet Banking
		8022021	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 87,00	IP166.852.432.762
Total					\$ 600,00	
26530356758	\$ 1.100,00	9022021	26530356758	Cuenta de ahorros de la cliente Susana Torio	\$ 240,00	Mobile Internet Banking
		13022021	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 860,00	IP166.852.432.762
Total					\$ 1.100,00	
26530356758	\$ 350,00	13022021	26530356758	Cuenta de ahorros de la cliente Susana Torio	\$ 350,00	IP166.852.432.762
Total					\$ 350,00	
Total traslados de Tarjeta de Crédito	\$ 7.144,85			Total de Pagos	\$ 7.144,85	

Conclusión: se han efectuado movimientos y traslados de saldos de las cuentas de la señora Susana Torio, a diferentes cuentas entre las que figuran un familiar del ejecutivo de ventas internas Elvis Nieto de Agencia San Benito.



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 13
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Revisión de Videos de Vigilancia	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		

Procedimiento: Solicitar los videos de vigilancia de la agencia San Benito en las fechas en que los clientes que han reclamado se han presentado a la sucursal para solicitar la creación de su usuario de banca en línea y así monitorear si ha habido irregularidades en el proceso

Este día se realizó la revisión de los videos de videovigilancia de la agencia de BANDECA ubicada en Colonia San Benito Bulevar del Hipódromo 665 San Salvador con el fin de verificar si los clientes que han presentado reclamo al banco se han presentado a las instalaciones del banco a realizar diferentes tramites en las fechas y horas que se han registrado en el sistema.

En los videos revisados se observa que la cliente Susana Torio no estaba presente en las instalaciones del banco a la hora y fecha en que se creó el usuario de banca online y en la fecha en que se realizó tramite de crédito móvil 777000024397 desde la IP 166.852.432.762 y es de mencionar que ella no tiene acceso al equipo desde donde se realizaron estos trámites dado que el dueño es el banco.

En los videos revisados se observa que a la hora y fecha que se realizan transacciones de retiro sin tarjeta por la cliente Susana Torio, es el ejecutivo Elvis Nieto es quien hace esos retiros



Conclusión

Se reviso los videos de vigilancia del banco y verificamos que la señora Susana Torio no se encontraba en las instalaciones del banco a la hora y fecha en que se creó el usuario de banca en línea ni cuando se solicitó el crédito móvil, sin embargo, pudimos observar al ejecutivo Elvis Nieto realizando retiros sin tarjeta a la hora y fecha en que se registra que la cliente Susana Torio realiza esas transacciones



ADVISORS INTERNATIONAL, S.A. DE C.V.

REF. **PT 14****Cliente:** BANDECA S.A.**Preparado por** N.S.**Cedula:** Revisión de Base de Datos Área de Call Center**Revisado por** V.C.**Periodo:** Del 1 de enero de 2020 al 30 de junio de 2021

Procedimiento: Revisar base de datos del área de call center de BANDECA para determinar el registro de llamadas realizadas y recibidas por los clientes que han realizado reclamo al banco, así como fechas y horas en que se realizaron y Solicitar las grabaciones de las llamadas

Este día se realizó la revisión de la base de datos del área de call center de BANDECA con el fin de identificar si hay registros de llamadas entrantes y salientes que estén relacionadas con clientes que han presentado reclamo al banco

Como resultado de esta revisión, no se encontraron registros de llamadas entrantes y salientes de los números del banco con relación a los clientes que han presentado reclamo al banco

Reg de Llamadas	Tipo	Número	Fecha	Duración
421	Saliente	13...	03/03/5877521 -596-8-...	00:09
1	Perdida	13...	03/03/5877521 -596-8-...	--
1	Perdida	13...	03/03/5877521 -596-8-...	--
13	Saliente	13...	03/03/5877521 -596-8-...	00:36
311	Entrante	13...	03/03/5877521 -596-8-...	01:09
14	Saliente	13...	03/03/5877521 -596-8-...	--
64	Entrante	13...	03/03/5877521 -596-8-...	01:18
26	Saliente	13...	03/03/5877521 -596-8-...	00:13
14	Saliente	13...	03/03/5877521 -596-8-...	--
19	Entrante	1300000000	03/03/5877521 -596-8-...	00:20
23	Entrante	13...	03/03/5877521 -596-8-...	00:36
13	Entrante	13...	03/03/5877521 -596-8-...	01:09
2	Entrante	13...	03/03/5877521 -596-8-...	00:24

Conclusión

No se encontraron llamadas entrantes y salientes registradas en el sistema de call center del banco, que tengan relación con el caso de la cliente Susana Torio. La señora se comunicaba directamente al número de celular del ejecutivo Elvis Nieto cuando tenía alguna consulta



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 15
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Revisión de Correos Electrónicos	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		
Procedimiento:	Revisar los correos electrónicos del área de call center del banco, recibidos y enviados que tengan relación con los clientes que han presentado reclamo al banco		

BANDECA

BANCO DE DESARROLLO CENTROAMERICANO

1 mensaje

CREACION DE USUARIO EN BANCA EN LINEA

15 de Agosto de 2020 a la hora
11: 50 a. m.

Responder a: No contestar a este correo < infobandeca@bandeca.sv >

Para: Susana Torio < susanatorio2020@gmail.com >

Estimado Cliente: Susana Torio

Le informamos que su usuario de banca en linea ha sido creado con exito
Su usuario de banca en linea es: 090909091

[Ver el mensaje en su contexto](#)

[Modifique sus preferencias de suscripción](#)

Reading this in an email? [Download the mobile app and receive notifications on your mobile device.](#)

BANDECA

BANCO DE DESARROLLO CENTROAMERICANO

1 mensaje

INFORMACION SOBRE CREDITO MOVIL

5 de Septiembre de 2020 a la hora
8: 20 a. m.

Responder a: No contestar a este correo < infobandeca@bandeca.sv >

Para: Susana Torio < susanatorio2020@gmail.com >

Estimado Cliente: Susana Torio

Le informamos que su credito movil solicitado a sido aprobado
El desembolso del credito sera depositado a la cuenta de ahorros N° 026530356758

[Ver el mensaje en su contexto](#)

[Modifique sus preferencias de suscripción](#)

Reading this in an email? [Download the mobile app and receive notifications on your mobile device.](#)

Conclusión

Se reviso los correos electrónicos de atención al cliente de BANDECA encontrando únicamente dos correos asociados al caso de la cliente Susana Torio, el primer correo se le envió para hacerle saber que se había creado un usuario a su nombre en la banca en línea del banco y el segundo para notificarle sobre el crédito móvil que había solicitado, mencionar que este correo encontrado no corresponde al que se tiene en los registros de la señora Susana Torio por lo que se concluye que fue creado para asociarlo cuando se creó el usuario de banca en línea



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 16
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Entrevista a Cliente	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		
Procedimiento:	Entrevistar a uno de los clientes que ha sido afectado para saber el procedimiento que realizó en la captación de datos personales por parte de BANDECA		

ENTREVISTA A CLIENTE

FECHA: 25 de agosto de 2021

NOMBRE DEL ENTREVISTADO: Susana Torio

LUGAR DE LA ENTREVISTA: Centro Financiero de BANDECA

Saludo: Buenas tardes mi nombre es Nelson Gabriel Sánchez y estamos realizando una investigación sobre el fraude a través de robo de identidad a clientes en la entidad bancaria En este sentido es importante su opinión sincera con respecto a las preguntas que le realizaremos

1. ¿Cuánto tiempo lleva siendo cliente de esta entidad bancaria?

Tengo 4 años de ser cliente de este banco

2. ¿Qué productos o servicios a solicitado y con quien los ha solicitado?

he solicitado cuenta de ahorros, créditos y tarjetas de crédito y débito

3. ¿Recibió usted alguna llamada del ejecutivo de negocios el sr. Elvis Nieto para consultarle sobre algún crédito que quisiera solicitar?

Si, el me llamo para proponerme un crédito de consolidación de otro préstamo que tenía pendiente, yo acepte esa consolidación

4. ¿Solicito usted la creación de banca en línea?

Yo no recuerdo haber solicitado la banca en línea, porque yo le dije al sr. Elvis que yo no sé usar eso

5. ¿Solicito usted cambio de número de teléfono en los documentos de registro del banco?

No, yo sigo teniendo el mismo número desde que hice los primeros tramites en el banco ese mismo número tengo no lo he cambiado

6. ¿Solicito usted un crédito móvil con el ejecutivo de negocios el sr. Elvis Nieto?

No, yo no he solicitado ningún crédito móvil, solo el que me ofreció para lo de la consolidación

7. ¿De qué manera se comunicaba usted con el banco? ¿Por correo, por teléfono?

Pues el sr. Elvis me había dado su número de celular y yo ahí le llamaba si tenía alguna consulta

8. De qué manera se dio cuenta de transacciones inusuales en su cuenta bancaria?

Me di cuenta porque empecé a ver operaciones en mi cuenta de ahorros que yo no había realizado

9. Firmo usted documentos del banco sin leerlos?

Pues la verdad que yo tenía bastante confianza en el sr. Elvis porque nunca me había quedado mal y algo que yo solicitara y el cada vez que hacía algún trámite me decía que firmara varios papeles que la verdad yo no sabía para que eran y yo los firmaba porque confiaba en él, también él me decía que le prestara el teléfono y yo se lo prestaba

10. Consulto usted con el banco por las transacciones inusuales que detecto en su cuenta bancaria

Si, yo le llamé al señor Elvis y él me dijo que eran errores del sistema, y al ver que seguían registrándose transacciones que yo no había hecho me fui para el banco a hacer el reclamo ahí me atendieron y me dijeron que iban a investigar

Conclusión

Se entrevisto a la cliente Susana Torio en las instalaciones del banco, quien manifestó que el ejecutivo Elvis Nieto la contacto para realizar un crédito de consolidación a lo cual ella acepto, pero no recuerda haber tramitado la creación de banca en línea ya que el ejecutivo le hacía firmar documentos y ella no sabía de qué eran y de igual forma él le decía que le prestara el teléfono y ella se lo prestaba porque le tenía confianza



ADVISORS INTERNATIONAL, S.A. DE C.V.

Hoja No. 1 de 1

Tipo de Auditoria:	Forense	REF.	PT 17
Cliente:	BANDECA S.A.	Preparado por	N.S.
Cedula:	Entrevista a Ejecutivo de Negocio	Revisado por	V.C.
Periodo:	Del 1 de enero de 2020 al 30 de junio de 2021		
Procedimiento:	Entrevistar al ejecutivo de ventas involucrado en el caso para analizar sus interacciones con los clientes afectados		

ENTREVISTA A EJECUTIVO DE NEGOCIO

FECHA: 26 de agosto de 2021

NOMBRE DEL ENTREVISTADO: Elvis Nieto

LUGAR DE LA ENTREVISTA: Instalaciones de BANDECA

Saludo: Buenas tardes mi nombre es Nelson Gabriel Sánchez y estamos realizando una investigación sobre el fraude a través de robo de identidad a clientes en la entidad bancaria. En este sentido es importante su opinión sincera con respecto a las preguntas que le realizaremos.

1. ¿Cuánto tiempo lleva desempeñando el cargo de ejecutivo de negocios en esta entidad bancaria?

Tengo 6 años de trabajar aquí como ejecutivo de negocios.

2. Conoce usted a la señora Susana Torio?

Si, ella es cliente del banco y ha solicitado varios productos con mi persona.

3. Desde hace cuánto tiempo la señora Susana Torio ha solicitado productos o servicios financieros con usted

Desde hace como 4 años.

4. Que tipos de productos ha solicitado

Ha solicitado tarjetas de crédito, préstamos bancarios y la cuenta de ahorros.

5. Solicito la señora Susana Torio la creación de banca en línea con usted

No, fui yo quien hizo que firmara la autorización y yo cree la banca en línea con las credenciales de la señora.

6. Solicito usted un crédito móvil a nombre de la señora Susana Torio por medio de banca en línea?

Si yo solite el crédito móvil con las credenciales de la señora sin su autorización

7. Los traslados de saldos de las tarjetas de crédito a nombre de la señora Susana Torio a las cuentas de ahorro fueron realizados por usted?

Si, yo realice esos traslados y realice pagos y traslados a mi cuenta de ahorros y a cuenta de mi papá

8. Los cambios de teléfono registrados en el sistema fueron realizados por usted?

Si, yo cambie el número de teléfono y registre un número que yo tenia

9. En algún momento la señora Susana Torio se comunicó con usted para consultarle transacciones inusuales en su cuenta de ahorros

Si ella me llamo y yo le dije que eran errores del sistema

10. De qué manera perfilo a las personas para realizar transacciones bancarias sin su consentimiento

Las perfile que fueran personas de edad porque sé que no entienden mucho de la tecnología y también por la confianza que tenían en mi

11. A parte de la señora Susana Torio ha realizado transacciones a nombre de otras personas sin su consentimiento

Si realice operaciones con dos clientes más a parte de la señora Susana Torio

El señor Armando Puentes y la señora Elena Nito.

Conclusión

Se consulto al ejecutivo Elvis Nieto mediante una entrevista sobre el crédito móvil a nombre de la señora Susana Torio a lo cual respondió que él había realizado transacciones a nombre de la señora sin su consentimiento, también que había realizado traslados entre tarjetas de crédito y cuentas de ahorro, que cambio números de teléfono, que las transacciones las realizo desde la banca en línea, que además de la señora Susana Torio habían dos clientes más a los cuales había realizado transacciones sin su consentimiento

3.15 Presentación de los resultados de la auditoria

INFORME DE AUDITORÍA FORENSE

BANDECA, S.A.

Señores:

Junta General de Accionistas

Junta Directiva

BANDECA S.A.

Presente.

Fuimos contratados para realizar una auditoría forense, enfocada a esclarecer si uno o más de los empleados que laboran en la entidad financiera BANDECA S. A. se han apropiado y retenido dinero de los clientes de la entidad bancaria a través de robo de identidad

Parte responsable de la información sujeta a auditoría forense

La información sujeta a examen de la auditoría forense realizada fue proporcionada por la gerencia de la entidad financiera BANDECA, S. A., de la cual el área negocios es la responsable del asunto principal sujeto a investigación; quienes proporcionaron las evidencias soportadas en registros de vinculaciones, análisis de estudios crediticios y demás documentos subyacentes al caso sujeto a auditoría.

Responsabilidad de los auditores forenses

Fuimos contratados para realizar una auditoría forense y esclarecer si se están cometiendo actos ilícitos en el área de negocios de la entidad financiera BANDECA, S.A., con el propósito de emitir un informe que muestre los resultados obtenidos, mediante conclusiones, sobre los siguientes puntos de auditoría:

- Determinar los hechos relacionados con el trámite de crédito móvil No. 777000024397 y retiros en efectivo de tarjetas de crédito y débito a nombre de la cliente Susana Torio
- Determinar si existió violación a las políticas y procedimientos aprobados por BANDECA S.A.
- Determinar si existe evidencia para remitir los casos a las autoridades judiciales.

Identificación de las normas bajo las cuales se preparó este informe

Este encargo se condujo con la norma NIEA 3000 (Revisada) Encargos de Aseguramiento Distintos de la Auditoría o de la Revisión de Información Financiera Histórica, Marco Internacional de Encargos de Aseguramiento y las Modificaciones de Concordancia de Otras NIEA. Esta Norma comprende los trabajos para atestiguar con seguridad razonable y los trabajos para atestiguar con seguridad limitada.

Identificación de los criterios

Para el desarrollo del trabajo, fue necesario analizar y tomar de base, diversa y amplia cantidad de información y documentación, entre las que se encuentran:

- Información proporcionada por la entidad bancaria
- Documentación solicitada a BANDECA S.A.
- Referencias a leyes y normativas técnicas de auditoría
- Estudio y comprensión del control interno implementado en el área de negocios de la entidad
- Revisión de bitácora de transacciones electrónicas

- Revisión de sistemas informáticos relacionados a transacciones electrónicas
- Análisis de la información provista por la entidad bancaria relacionada con la auditoría.
- Revisión de huellas de auditoría

Limitaciones en el desarrollo del trabajo

Durante la realización de la auditoría forense no se presentó ninguna situación que limitará el desarrollo de procedimientos para la recolección de evidencia

Uso de este informe

Este informe ha sido preparado para uso exclusivo de la junta general de accionistas y junta directiva de BANDECA S.A.

Naturaleza de la denuncia y análisis preliminar.

El día El día 14 de enero de 2021 se recibió reclamo de la cliente Susana Torio, quien solicitó se investigue un crédito digital realizado en fecha 5 de septiembre de 2020, por un monto de \$4,245.00 el cual no ha solicitado además de los retiros efectuados en las tarjetas de crédito MasterCard 5369580000683783 y Visa débito 4550005050147086, dado que no los ha efectuado. Adicionalmente la cliente manifiesta que su cuenta de ahorro N.º 026530356758 registra abonos y retiros que ella no reconoce.

Con base al análisis preliminar identificamos las siguientes situaciones:

- Posible fraude en el trámite del crédito móvil 777000024397 y en los retiros de las tarjetas de crédito MasterCard 5369580000683783 y Visa débito 4550005050147086 a nombre de la cliente Susana Torio.
- Incumplimiento con los controles y políticas establecidas.

Resultados de la investigación.

Respecto al posible fraude en la colocación del crédito móvil 777000024397 y los retiros de las tarjetas de crédito MasterCard 5369580000683783 y Visa débito 4550005050147086 a nombre de la cliente Susana Torio, se determinó lo siguiente:

- Según el sistema MIQ C (sistema de evaluación de créditos) el ejecutivo de negocios Elvis Nieto, evaluó a la cliente Susana Torio, para tramitar dos créditos de consumos, los cuales fueron desembolsados en fecha 12 de octubre de 2020.
- El día 15 de agosto de 2020 según el sistema Inbase, la cliente Susana Torio solicitó el usuario de Banca Online, creándose el usuario 090909091 según los registros del archivo maestro de usuarios de la aplicación de internet banking. En esta misma fecha se registra que se efectuó el cambio de contraseña.
- En fecha 15 de agosto de 2020, según registros del archivo INTAS (bitácora de transacciones electrónicas), el usuario de Banca Online 090909091, asociado al NIU 253320647 de la cliente Susana Torio, registra que se efectuó cambio de contraseña desde la IP166.852.432.762 asignada al ejecutivo de negocios Elvis Nieto de Agencia San Benito, según detalle:

Usuario de Internet	Fecha	Hora	NIU	Descripción	IP donde se realizó el cambio
090909091	15/08/2020	12:24:43	253320647	Cambio de Contraseña	IP166.852.432.762

- Según registros del archivo INTAS (bitácora de transacciones electrónicas), el usuario de banca online 090909091, asociado al NIU 253320647 de la cliente Susana Torio, registra que previo a la apertura del crédito móvil se realizaron acciones desde la IP166.852.432.762 asignada al ejecutivo de negocios Elvis Nieto de Agencia San Benito, según detalle:

Usuario de Internet	Fecha	Hora	NIU	Descripción	IP donde se realizó el cambio
90909091	15/08/2020	8:20:44	253320647	Login exitoso	IP166.852.432.762
90909091	15/08/2020	8:21:16	253320647	Resumen de cuentas	IP166.852.432.763
90909091	15/08/2020	8:22:42	253320647	Salir	IP166.852.432.764
90909091	15/08/2020	8:26:23	253320647	Login fallido, contraseña errónea	IP166.852.432.765
90909091	15/08/2020	8:29:17	253320647	Login exitoso	IP166.852.432.766
90909091	15/08/2020	8:30:05	253320647	Salir	IP166.852.432.767
90909091	15/08/2020	13:27:32	253320647	Login exitoso	IP166.852.432.768
90909091	15/08/2020	13:36:48	253320647	Resumen de cuentas	IP166.852.432.769
90909091	15/08/2020	13:39:14	253320647	Confirmar teléfono y correo	IP166.852.432.770

- Se revisó el archivo INTAS (bitácora de transacciones electrónicas, según el usuario de banca online 90909091, asociado al NIU 253320647 de la cliente Susana Torio, la cual registra el ingreso de la Banca Online desde la IP166.852.432.762 asignada al ejecutivo Elvis Nieto de Agencia San Benito y registra trámite de crédito móvil 777000024397 por \$4,145.00. Según las cámaras de Agencia San Benito, a la hora del trámite del crédito no hay presencia de la cliente Susana Torio, y es de mencionar que ella no tiene acceso a dicho equipo, dado que el dueño es el Banco, a continuación, se detalla los registros del trámite de crédito móvil según archivos INTAS (bitácora de transacciones electrónicas)

Usuario de Internet	Fecha	Hora	NIU	Canal	Descripción	Monto	IP donde se realizó la transacción
90909091	15082020	10:01:54	253320647	Login	Login exitoso	0,00	IP166.852.432.762
90909091	15082020	10:02:03	253320647	Consultas	Resumen de cuentas	0,00	IP166.852.432.762
90909091	15082020	10:04:15	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	10:04:49	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	10:15:27	253320647	Logout	Salir	0,00	IP166.852.432.762
90909091	15082020	12:19:35	253320647	Login	Login exitoso	0,00	IP166.852.432.762
90909091	15082020	12:19:44	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	12:27:05	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	13:27:21	253320647	Logout	Salir	0,00	IP166.852.432.762
90909091	15082020	14:45:09	253320647	Login	Login exitoso	0,00	IP166.852.432.762
90909091	15082020	14:45:48	253320647	Servicios Bancarios	Registro de Ingreso a Productos Móviles	0,00	IP166.852.432.762
90909091	15082020	14:57:29	253320647	Servicios Bancarios	Crédito móvil desembolsado (exitoso)	4,145,00	IP123.000.000.009

- El desembolso del crédito móvil está parametrizado para que se efectuó a una cuenta de la cliente que lo tramita, por lo que el monto neto del crédito móvil 777000024397, por \$4,150.00, se abonó a la cuenta de ahorros 026530356758 a nombre de la cliente Susana Torio. Posteriormente al desembolso, el usuario de Banca Online 90909091, asociado al NIU 253320647 de la cliente Susana Torio, registra ingreso a conexión personal desde la IP166.852.432.762 asignada al ejecutivo Elvis Nieto de Agencia San Benito, y registra que se realizaron traslados y pagos de tarjeta de crédito, según detalle:

Usuario	Fecha	Hora	Cuenta que se abonó con desembolso	Monto	IP donde se realizó la transacción
90909091	15082020	15:18:31	Tarjeta de Crédito 5369580000683783	1,500.00	IP166.852.432.762
90909091	16082020	10:07:25	de la cliente Susana Torio	824.30	IP166.852.432.762
90909091	18082020	12:21:43	Cuenta de ahorros 026530356758 de la cliente Susana Torio	1,500.00	IP166.852.432.762
Total				3,824.30	

Del desembolso por \$4,150.00 quedaron en la cuenta de ahorros 026530356758 de la cliente Susana Torio, un remanente de \$325.70 los cuales fueron utilizados por la cliente.

Respecto a los retiros de las tarjetas de crédito MasterCard 5369580000683783 y Visa débito 4550005050147086 a nombre de la cliente Susana Torio, se determinó lo siguiente:

- Según sistema Inbase, las tarjetas de crédito y débito han sido tramitadas por el ejecutivo Elvis Nieto, el 04/08/2020.
- Los registros del archivo INTAS (bitácora de transacciones electrónicas) el usuario 90909091, asociado al NIU 253320647 de la cliente Susana Torio, registra que entre sus tarjetas de crédito y débito se han realizado traslados a sus cuentas de ahorro, desde la IP166.852.432.762 asignada al ejecutivo Elvis Nieto de Agencia San Benito, según detalle:

Usuario	Fecha	Hora	Número de Tarjeta de Crédito / Débito	Cuenta de ahorros abonada	Monto	IP de donde se realizó la transacción
90909091	21/08/2020	13:34:21	5369580000683780	26530356758	\$ 1.200,00	IP166.852.432.762
90909091	21/08/2020	10:08:57	5369580000683780	26530356758	\$ 1.000,00	IP166.852.432.762
90909091	23/08/2020	8:22:13	5369580000683780	777000024397	\$ 200,00	IP166.852.432.762
90909091	23/08/2020	9:09:37	5369580000683780	777000024397	\$ 384,00	IP166.852.432.762
90909091	24/08/2020	8:50:03	5369580000683780	777000024397	\$ 275,00	IP166.852.432.762
90909091	04/01/2021	11:40:23	5369580000683780	777000024397	\$ 550,00	IP166.852.432.762
90909091	06/01/2021	11:53:04	5369580000683780	777000024397	\$ 500,00	IP166.852.432.762
90909091	10/01/2021	15:46:18	5369580000683780	777000024397	\$ 500,00	IP166.852.432.762
90909091	02/02/2021	17:05:29	5369580000683780	777000024397	\$ 700,00	IP166.852.432.762
90909091	08/02/2021	10:25:58	4550005050147086	26530356758	\$ 1.150,00	Mobile Internet Banking
90909091	10/02/2021	14:21:18	4550005050147086	26530356758	\$ 450,00	IP166.852.432.762
Total retiros en tarjetas de crédito y debito					\$6.909,00	

- En los registros del archivo INTAS (bitácora de transacciones electrónicas) el usuario 90909091, asociado al NIU 253320647 de la cliente Susana Torio, registra que posterior a los traslados de los saldos realizados en las tarjetas de crédito y débito a las cuentas de ahorros de la cliente se realizaron los siguientes pagos y transferencias según detalle:

Cuenta de ahorros que recibió abono de la tarjeta de crédito	Monto abonado	Fecha de transacción	Referencia Pagada	Nombre de Cliente de la referencia Pagada	Monto	IP donde se realizó la transacción
26530356758	\$ 1.210,85	15082020	4550005050147080	Tarjeta de débito de la cliente Susana Torio	\$ 32,85	IP166.852.432.762
		15082020	4456005465411567	Tarjeta de crédito de Ever Nieto (padre del ejecutivo Elvis Nieto)	\$ 270,00	IP166.852.432.762
		15082020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 908,00	IP166.852.432.762
Total					\$ 1.210,85	
26530356758	\$ 1.000,00	15082020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 1.000,00	IP166.852.432.762
Total					\$ 1.000,00	
777000024397	\$ 400,00	20082020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 400,00	IP166.852.432.762
Total					\$ 400,00	
777000024397	\$ 584,00	25102020	4550005050147080	Tarjeta de débito de la cliente Susana Torio	\$ 95,00	IP166.852.432.762
		25102020	Retiro Sin Tarjeta	Según video quién retira es ejecutivo Elvis Nie	\$ 270,00	Mobile Internet Banking
		25102020	Retiro Sin Tarjeta	Según video quién retira es ejecutivo Elvis Nie	\$ 219,00	Mobile Internet Banking
Total					\$ 584,00	
777000024397	\$ 250,00	4112020	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 250,00	IP166.852.432.762
Total					\$ 250,00	
777000024397	\$ 600,00	7122020	Retiro Sin Tarjeta	Según video quién retira es ejecutivo Elvis Nie	\$ 350,00	Mobile Internet Banking
		6012021	Retiro Sin Tarjeta	Según video quién retira es ejecutivo Elvis Nie	\$ 250,00	Mobile Internet Banking
Total					\$ 600,00	
777000024397	\$ 550,00	7012021	5369580000683783	Tarjeta de crédito de la cliente Susana Torio	\$ 50,00	IP166.852.432.762
		7012021	Retiro Sin Tarjeta	Según video quién retira es ejecutivo Elvis Nie	\$ 200,00	Mobile Internet Banking
		13012021	Retiro Sin Tarjeta	Según video quién retira es ejecutivo Elvis Nie	\$ 300,00	Mobile Internet Banking
Total					\$ 550,00	
777000024397	\$ 500,00	14012021	4456005465411567	Tarjeta de crédito de Ever Nieto (padre del ejecutivo Elvis Nieto)	\$ 250,00	IP166.852.432.762
		15012021	26650510887	Cuenta de ahorros de Elvis Nieto	\$ 250,00	IP166.852.432.762
Total					\$ 500,00	
777000024397	\$ 600,00	4022021	7771561564397	Préstamo móvil de la cliente Susana Torio	\$ 105,00	IP166.852.432.762
		4022021	5369580000683783	Tarjeta de crédito de la cliente Susana Torio	\$ 108,00	IP166.852.432.762
		5022021	26530356758	Cuenta de ahorros de la cliente Susana Torio	\$ 300,00	Mobile Internet Banking
		8022021	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 87,00	IP166.852.432.762
Total					\$ 600,00	
26530356758	\$ 1.100,00	9022021	26530356758	Cuenta de ahorros de la cliente Susana Torio	\$ 240,00	Mobile Internet Banking
		13022021	24653172648	Cuenta de ahorros de la cliente Elena Nito	\$ 860,00	IP166.852.432.762
Total					\$ 1.100,00	
26530356758	\$ 350,00	13022021	26530356758	Cuenta de ahorros de la cliente Susana Torio	\$ 350,00	IP166.852.432.762
Total					\$ 350,00	
Total traslados de Tarjeta de Crédito	\$ 7.144,85			Total de Pagos	\$ 7.144,85	

- El día 16 de febrero de 2021 se consultó al sistema IPS, observando que la cliente Susana Torio, registra el teléfono 61349687, el cual difiere con el número que registra la cliente en el Formulario de Conocimiento del Cliente del 30/09/2019 y en la solicitud de crédito 5246876 de fecha 5/09/2020, el cual es el 77459472.
- Revisamos las huellas de auditoría del periodo de enero de 2019 al 18 de febrero de 2021 observando que la cliente Susana Torio, no registra cuando se realizó el cambio del número telefónico 61139687.
- El 14 de marzo de 2021, en las instalaciones del Centro Financiero de BANDECA, se entrevistó a la cliente Susana Torio, quien manifestó que el ejecutivo Elvis Nieto le contactó para tramitarle un crédito de consolidación de deuda, a lo cual ella estuvo de

acuerdo y se lo desembolsaron, respecto a la banca electrónica no recuerda cómo fue que la tramitó, dado que el ejecutivo le hacía firmar documentos y ella no sabía de qué eran, y de igual forma él le decía que le prestara el teléfono y ella se lo entregaba porque confiaba en él.

- Los saldos en las cuentas de la cliente al 30 de marzo de 2021 son los siguientes:

Producto	Referencia	Saldo al 30/03/2021
Tarjeta de crédito	5369580000683783	\$ 3.510,40
Tarjeta de debito	4550005050147080	\$ 1.520,90
Crédito móvil	7771561564397	\$ 3.824,30
Cuenta de ahorro (cargos del crédito móvil)	26530356758	\$ 7,40
Cuenta de ahorro (saldo utilizado por la cliente)	26530356758	\$ 325,70
Total		\$ 9.188,70

- Se entrevistó al ejecutivo Elvis Nieto, sobre el trámite del crédito móvil quién manifestó lo siguiente:
 - Tramitó el crédito móvil de la cliente Susana Torio sin su consentimiento.
 - Que realizó traslados de las tarjetas de crédito y débito de la cliente Susana Torio, a las cuentas de ahorro sin autorización de la cliente.
 - La cliente Susana Torio, le consultó sobre las operaciones que registraba en la cuenta de ahorros y que él le manifestó que eran errores de sistema.
 - El sistema MIG C efectuó cambios de teléfono de los clientes, registrando el teléfono 61349687 y 77528839, los cuales son de su propiedad.
 - Las transacciones fueron realizadas a través de la banca online con las credenciales de los clientes sin su consentimiento
 - Realizó retiros de efectivo sin tarjeta
 - Los clientes los perfiló por la confianza que ellos le tenían

- Existen 2 clientes más con los que ha realizado el mismo procedimiento, los clientes son los siguientes:

- Armando Puentes
- Elena Nito

Conclusiones de los auditores forenses

Basados en la evidencia documental y testimonial concluimos que el ejecutivo de negocios Elvis Nieto modificando el teléfono de 3 clientes registrando el teléfono 61349687 (teléfono del ejecutivo de negocios) lo que le permitió la recuperación de la clave de conexión personal de banca en línea y por este medio realizar transferencias de tarjeta de crédito hacia las cuentas de los clientes y realizar solicitudes de crédito móvil. con los fondos transferidos a la cuenta de los clientes realizar retiros en ATM a través de la modalidad de retiro sin tarjeta, transferencia a su cuenta y pagos a las tarjetas de crédito defraudadas. Mecanismo utilizado para operar, confianza, perfil de cliente, exclusividad de atención del ejecutivo.

Por lo antes expuesto se recomienda:

- La Dirección de Banca de Personas en conjunto con la Dirección Legal deberá evaluar los resultados del informe, para procesar judicialmente con los involucrados relacionados al caso de fraude.
- La Subgerencia de Operaciones de Agencias en conjunto con el Área Legal deben informar a los clientes sobre la resolución del caso.

Recomendaciones

Respecto al control interno de los procesos de actualización de información de clientes recomendamos lo siguiente:

- Revisar el proceso de actualización de datos (teléfonos y correos) y asegurarse que todos los cambios realizados en todos los canales queden registrados en las huellas de auditoría.
- Implementar controles que permitan monitorear las tarjetas de crédito que el cliente ha devuelto.

San Salvador, a los 20 días del mes octubre de 2021.


Vilma Yesenia Caceres Guevara

Socio del encargo

Registro No 4040



4. CONCLUSIONES

Basados en la investigación realizada y en los resultados obtenidos, en orden de prioridad concluimos los siguiente:

- a) La tecnología en el Sistema Bancario Salvadoreño está ganando terreno en las operaciones diarias de los usuarios, por consiguiente, existe un alto grado de riesgo de fraude financiero por robo de identidad, y las personas más expuestas a ser víctimas de este tipo de delitos siempre serán las que tengan menos conocimiento informático y menos capacidad de operar dispositivos inteligentes.
- b) Una correcta elaboración de programas de auditoría, desde su planeación hasta su ejecución, cimentada en una estrategia de detección de fraude y en la utilización de técnicas especializadas en el robo de identidad hará que la detección de los puntos clave de la investigación sea efectiva y por consiguiente su informe concluyente sea de relevancia para las instancias judiciales.
- c) La capacitación constante sobre temas de fraude por robo de identidad en todas sus formas es de vital importancia para los profesionales ejercientes debido al aumento de casos de este delito en los últimos años, así como también el conocimiento de las distintas normas técnicas y legales nacionales e internacionales que acompañan a este tipo de delitos.

5. RECOMENDACIONES

A continuación, brindamos algunas recomendaciones con el objetivo de aportar alternativas para el mejoramiento de las condiciones del auditor forense ante casos de robo de identidad a través de la banca electrónica en el Sistema Bancario Salvadoreño:

- a) A los contadores públicos y auditores internos, tener en cuenta la Ley de Bancos, toda la normativa técnica establecida por el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría, así como también las políticas de cada una de las entidades bancarias para incluir programas internos que ayuden a la prevención de estos delitos.
- b) A los auditores forenses, mantenerse actualizados con los cambios que puedan darse en la normativa técnica que rige la auditoría forense y las distintas leyes especiales que surjan entorno a los casos de robo de identidad a través de medios electrónicos, como por ejemplo la Ley Especial Contra los Delitos Informáticos y Conexos, y a velar por una mayor preparación en el área.
- c) A las universidades salvadoreñas, hacer una revisión de las asignaturas correspondientes a la carrera de Contaduría Pública, con el fin de incluir la auditoría forense en su programa, así como también crear espacios de aprendizaje a través de conferencias o especializaciones en el área de delitos electrónicos y afines, para contribuir al desarrollo de los profesionales que puedan enfrentarse a estos casos en el futuro.

BIBLIOGRAFÍA

Asamblea Legislativa. (1997). *Código Penal de El Salvador* (Decreto N° 1030 ed.).
<https://www.asamblea.gob.sv/sites/default/files/documents/decretos/C0AB56F8-AF37-4F25-AD90-08AE401C0BA7.pdf>

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR.
 (26/02/2016). *LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS*.
https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf

ASAMBLEA LEGISLATIVA- EL SALVADOR. (1999, 09 02). *Ley de Bancos*.
<https://www.asamblea.gob.sv/decretos/details/345>

BCR - GOBIERNO DE EL SALVADOR. (n.d.). *Regulaciones del Sistema Financiero*. Normas Vigentes.
<https://www.bcr.gob.sv/regulaciones/normas.php?mercado=&pagina=24¶m=ab3dc26437063f5a04600ee0439408c4&idMercado=&idEntidad=&tipoRegulacion=&palabra=&buscar=buscar>

Condusef. (n.d.). *Condusef atendió 802 reclamos por robo de identidades en abril*. Milenio. <https://www.milenio.com/negocios/condusef-atendio-802-reclamos-robo-identidades-abril>

IAASB. (2018). *Norma Internacional de Encargos de Aseguramiento 3000* (Vol. Encargos de Aseguramiento Distintos de la Auditoría o de la Revisión de Información Financiera Histórica). <https://www.ifac.org/system/files/publications/files/NIEA-3000-Revisada-Encargos-de-Aseguramiento-distintos-de-la-Auditoria-o-de-la-Revision-de-Informacion-Financiera-Historica-Marco-Internacional-de-Enc.pdf>

IFAC. (15/12/2009). *NORMA INTERNACIONAL DE AUDITORÍA 315 IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS DE INCORRECCIÓN MATERIAL MEDIANTE EL CONOCIMIENTO DE LA ENTIDAD Y DE SU ENTORNO*. IAASB.
<http://www.aplicaciones-mcit.gov.co/adjuntos/niif/15%20-%20NIA%20315.pdf>

ORGANO LEGISLATIVO. (n.d.). *LEY REGULADORA DEL EJERCICIO DE LA CONTADURÍA*. http://www.oas.org/juridico/spanish/mesicic3_slv_contaduria.pdf

Suarez Beltran, E. A. (2018).

https://repository.ucc.edu.co/bitstream/20.500.12494/7980/1/2018_auditoria_deteccion_fraud_e.pdf

UNIVERSIDAD DE EL SALVADOR, Campos Garay, S. S., Cuéllar Reyes, G. M., & Segovia Monjaras, W. A. (2009). *Guía práctica para efectuar auditoría forense en las empresas comerciales de electrodomésticos de la ciudad de San Miguel*.

<http://opac.fmoues.edu.sv/infolib/tesis/50107349.pdf>

UNIVERSIDAD POLITECNICA SALESIANA, Sarango, M., & Tipan, P. (2014, Septiembre). *Análisis de la Auditoria Forense como método de prevención del fraude en las cooperativas de ahorro y crédito del distrito metropolitano en Quito*.

<https://dspace.ups.edu.ec/bitstream/123456789/7148/1/UPS-QT06041.pdf>

ANEXOS

Guía de preguntas para entrevista

1. ¿Cuál es el rol del auditor forense en los casos de fraude financiero a través del robo de identidad?
2. ¿Ha tenido alguna experiencia en casos de robo de identidad por medio de la banca electrónica? ¿Cuáles han sido los puntos clave de la investigación?
3. ¿Posee usted alguna especialización de auditoría forense en temas como fraude financiero y lavado de dinero?
4. ¿Qué tipo de técnicas forenses conoce que puedan ser aplicadas a casos de fraude financiero por robo de identidad en la banca electrónica salvadoreña?
5. ¿Considera usted que la normativa técnica con que se cuenta a nivel nacional en relación a la auditoría forense es funcional para desarrollar este tipo de casos?
6. ¿Cree que la legislación salvadoreña es lo suficientemente rígida para penalizar este tipo de delitos?
7. En su opinión, ¿Cuáles son las principales falencias en el Sistema Bancario Salvadoreño que aumentan el riesgo de fraude financiero por robo de identidad?
8. ¿Cuál es el perfil de los victimarios en este tipo de fraude que usted ha podido observar?
9. ¿Qué áreas de conocimiento cree que necesitaría reforzar para mejorar sus habilidades como auditor forense para la detección de este tipo de delitos?
10. ¿Qué tipos de controles internos aconsejaría implementar a las instituciones bancarias para minimizar el riesgo de fraude financiero por robo de identidad?

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

ENTREVISTA DIRIGIDA A: Antonio Cruz (Licenciado en Contaduría Pública)

1. *¿Cuál es el rol del auditor forense en los casos de fraude financiero a través del robo de identidad?*

De acuerdo al grado de experiencia que tengo en esta área de fraude puede decirse que apoyar en la resolución de un caso judicial, o por requisición de un cliente que necesite detectar actos de fraude por indicios que se han detectado, lo que es el robo de identidad como tal imagino que puede referirse a la suplantación que le hacen a la víctima y tener beneficios económicos en perjuicio de esta.

2. *¿Ha tenido alguna experiencia en casos de robo de identidad por medio de la banca electrónica? ¿Cuáles han sido los puntos clave de la investigación?*

No he tenido la oportunidad de llevar una auditoría que genere esta revisión como tal, unos posibles puntos clave es el registro de la documentación, revisión de los involucrados, posible incremento patrimonial, cálculo de transacciones cuestionables entre otras.

3. *¿Posee usted alguna especialización de auditoría forense en temas como fraude financiero y lavado de dinero?*

A la fecha solo recibo capacitaciones de lo que es el Lavado de Dinero y Financiamiento al Terrorismo, con la auditoría forense solo conozco a base de algunas capacitaciones que imparten las Escuela de Contadores Públicos, entre otros.

4. *¿Qué tipo de técnicas forenses conoce que puedan ser aplicadas a casos de fraude financiero por robo de identidad en la banca electrónica salvadoreña?*

Pienso que se aplican las técnicas generales de cualquier auditoria, pero se hace un énfasis en las situaciones que de acuerdo con la experiencia del auditor pueden representar riesgos de hechos de corrupción, ya sea discrepancia en los registros contables o inconsistencia en la documentación de las licitaciones

5. *¿Considera usted que la normativa técnica con que se cuenta a nivel nacional en relación a la auditoría forense es funcional para desarrollar este tipo de casos?*

Creo que debe ir cambiando poco a poco, las nuevas tecnologías de información se encuentran en un constante cambio por lo que es necesario que la normativa técnica aplicable se encuentre en función para poder desarrollar auditorias forenses.

6. *¿Cree que la legislación salvadoreña es lo suficientemente rígida para penalizar este tipo de delitos?*

La legislación salvadoreña debe modificarse para acelerar los procesos judiciales más rápido, en mi opinión las sanciones impuestas deben estar penalizadas en función de los delitos que se cometan.

7. En su opinión, ¿Cuáles son las principales falencias en el Sistema Bancario Salvadoreño que aumentan el riesgo de fraude financiero por robo de identidad?

Posiblemente sea por los sistemas que utilizan, muchas veces son inestables y pueden ser vulnerados, también por las personas que trabajan en estas organizaciones ya que los delitos pueden generarse internamente, y perjudica la imagen pública de la entidad.

8. ¿Cuál es el perfil de las víctimas y victimarios en este tipo de fraude que usted ha podido observar?

La mayoría de las víctimas son personas de la tercera edad, que por falta de conocimiento no saben utilizar sus dispositivos móviles, o saber sus accesos a cuentas ya que ahora todos podemos acceder a la Banca en Línea y muchas veces ellos son los más vulnerables. También las personas que aceptan obsequios o regalos certificados y entregan sus datos personales ya que estos son muchas veces claves para tener acceso a sus cuentas bancarias. Y en el caso de los que cometen el delito son personas con bastante conocimiento informático y que muy probablemente han estado laborando en alguna institución bancaria, puesto que se saben cada proceso a detalle y encuentran la forma de operar para sacar ventaja.

9. ¿Qué áreas de conocimiento cree que necesitaría reforzar para mejorar sus habilidades como auditor forense para la detección de este tipo de delitos?

Pienso que el conocimiento de técnicas de auditoría forense me es necesario, así como la capacidad de análisis de las situaciones que se vayan presentando y conocer una normativa técnica más específica enfocado en lo forense.

10. ¿Qué tipos de controles internos aconsejaría implementar a las instituciones bancarias para minimizar el riesgo de fraude financiero por robo de identidad?

Protocolos de investigación interna, también los protocolos de aplicación y rendición de cuentas, protocolos de acciones correctivas, debidas diligencias ampliadas, controles de riesgo de fraudes específicos por procesos, entre otros.

FICHAS BIBLIOGRAFICAS

Nombre del autor: Asamblea Legislativa de El Salvador

Fecha: 1997

Título: CODIGO PENAL DE EL SALVADOR

Sitio: Asamblea Legislativa de El Salvador

Consultado: 05/05/2021

Fuente: <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/C0AB56F8-AF37-4F25-AD90-08AE401C0BA7.pdf>

Nombre del autor: Asamblea Legislativa de El Salvador

Fecha: (26/02/2016).

Título: LEY ESPECIAL CONTRA DELITOS INFORMATICOS Y CONEXOS

Sitio: Asamblea Legislativa de El Salvador

Consultado: 10/05/2021

Fuente: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf

Nombre del autor: Asamblea Legislativa de El Salvador

Fecha: (02/09/1999).

Título: LEY DE BANCOS

Sitio: Asamblea Legislativa de El Salvador

Consultado: 11/05/2021

Fuente: <https://www.asamblea.gob.sv/decretos/details/345>

Nombre del autor: Banco Central de Reserva de El Salvador

Fecha:

Título: Regulaciones del Sistema Financiero

Sitio: Banco Central de Reserva de El Salvador

Consultado: 19/06/2021

Fuente: <https://www.bcr.gob.sv/regulaciones/normas.php?mercado=&pagina=24¶m=ab3dc26437063f5a04600ee0439408c4&idMercado=&idEntidad=&tipoRegulacion=&palabra=&buscar=buscar>

Nombre del autor: Milenio

Fecha: 14/06/2021

Título: Conducef atendió 802 reclamos por robo de identidad en abril

Sitio: MILENIO

Consultado: 25/06/2021

Fuente: <https://www.milenio.com/negocios/conducef-atendio-802-reclamos-robo-identidades-abril>

Nombre del autor: IAASB

Fecha: 2018

Título: Norma Internacional de Encargos de Aseguramiento 3000

Sitio: IFAC

Consultado: 25/06/2021

Fuente: <https://www.ifac.org/system/files/publications/files/NIEA-3000-Revisada-Encargos-de-Aseguramiento-distintos-de-la-Auditoria-o-de-la-Revision-de-Informacion-Financiera-Historica-Marco-Internacional-de-Enc.pdf>

Nombre del autor: IAASB

Fecha: (15/12/2009).

Título: NORMA INTERNACIONAL DE AUDITORÍA 315 IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS DE INCORRECCIÓN MATERIAL MEDIANTE EL CONOCIMIENTO DE LA ENTIDAD Y DE SU ENTORNO

Sitio: IFAC

Consultado: 25/06/2021

Fuente: <http://www.aplicaciones-mcit.gov.co/adjuntos/niif/15%20-%20NIA%20315.pdf>

Nombre del autor: Asamblea Legislativa de El Salvador

Fecha:2000

Título: LEY REGULADORA DEL EJERCICIO DE LA CONTADURIA

Sitio: Asamblea Legislativa de El Salvador

Consultado: 26/06/2021

Fuente:https://www.asamblea.gob.sv%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Fdecretos%2FDBCA1E61-7C37-4BFD-B821-3CFD146F702D.pdf&usg=AOvVaw0_AbwwpFNFLrxduKjUkB2

Nombre del autor: Campos Garay, S. S., Cuéllar Reyes, G. M., & Segovia Monjaras

Fecha:2009

Título: Guía práctica para efectuar auditoría forense en las empresas comerciales de electrodomésticos de la ciudad de San Miguel

Sitio: Repositorio Institucional de la Universidad de El Salvador

Consultado: 28/06/2021

Fuente: <http://opac.fmoues.edu.sv/infolib/tesis/50107349.pdf>

Nombre del autor: Sarango, M., & Tipan, P.

Fecha: septiembre 2014

Título: Análisis de la Auditoria Forense como método de prevención del fraude en las cooperativas de ahorro y crédito del distrito metropolitano en Quito

Sitio: Asamblea Legislativa de El Salvador

Consultado: 28/06/2021

Fuente:<https://dspace.ups.edu.ec/bitstream/123456789/7148/1/UPS-QT06041.pdf>