**UNIVERSIDAD DE EL SALVADOR**

**FACULTAD DE CIENCIAS ECONÓMICAS**

**TRABAJO DE GRADO DE ESPECIALIZACIÓN EN: AUDITORÍA FORENSE**

# "UTILIZACIÓN DE LAS HERRAMIENTAS SUPTECH Y REGTECH EN LA REALIZACIÓN DE AUDITORÍA FORENSE APLICADA A EMPRESAS FINTECH"


**PRESENTADO POR:**

| | |
|---|---|
| Moreno Aquino, Eunice Lisbeth | L10802-1994 |
| Rivera Carrillo, Noé Aquiles | L10802-1994 |
| Vásquez Berciano, Metzi Danelia | L10802-1994 |


**Mayo 2022**

**SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA**

AUTORIDADES CENTRALES

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

AUTORIDADES DE LA FACULTAD

| | |
|---|---|
| Decano de la Facultad de Ciencias Económicas | : Msc. Nixon Rogelio Hernández Vásquez. |
| Secretaria de la Facultad de Ciencias Económicas | : Licda. Vilma Marisol Mejía Trujillo. |
| Director de la Escuela de Contaduría Pública | : Lic. Gilberto Díaz Alfaro. |
| Coordinador General de Seminario de Graduación | : Lic. Mauricio Ernesto Magaña Menéndez. |
| Coordinador de Seminario de Proceso de Graduación de la Escuela de Contaduría Pública | : Lic. Daniel Nehemias Reyes López. |
| Docente Director | : Lic. Carlos Nicolás Fernández Linares. |
| | : Lic. José Ángel García Rodríguez. |
| Jurado Examinador | Lic. Jorge Luis Martínez Bonilla. |
| | Lic. Carlos Ernesto Ramírez. |

Mayo 2022

San Salvador, El Salvador Centro América.

## AGRADECIMIENTOS

Agradezco primeramente a Jehová Dios Todopoderoso por darme la vida, la guía, la sabiduría y por enseñarme sus principios y valores que nos permiten ser mejores personas cada día, agradezco también a mi mamá Reina Isabel Aquino Luna, quien siempre nos ha dado lo mejor de ella, se ha sacrificado por darnos todo lo que tenemos y apoyarnos en toda nuestra carrera, por siempre confiar en nosotros y ayudarnos en cada momento de nuestra vida, así mismo agradezco mucho a mi mami Francisca Luna y mi papi Wilfredo Aquino, quienes siempre nos apoyaron y nos amaron incondicionalmente y ayudaron a nuestra mamá a poder tener su propio logro, que hoy nos permite a nosotros también poder culminar esta meta, agradezco mucho también a mi hermano por tenerme paciencia y apoyarme en todo lo que ha estado a su alcance, todos ellos han sido mi mayor motivación para poder alcanzar esta meta, además agradezco mucho todo el apoyo que he recibido de Omar Alvarado en los últimos años con mucho amor, agradezco a mi equipo de especialización quienes han aportado sus conocimientos y habilidades para que todos podamos terminar este trabajo de la mejor manera, así mismo agradezco a los docentes que me forjaron a lo largo de mi carrera y que me brindaron sus conocimientos, habilidades y experiencias. Muchas gracias.

***Eunice Lisbeth Moreno Aquino.***

Agradezco a Dios, por bendecirme, guiarme, darme la sabiduría y el entendimiento. A mi madre Santísima, quien me ha cubierto con su manto divino. Agradezco a mis padres quienes desde pequeño me inculcaron los valores y principios que me definen como persona, por darme su apoyo incondicional a pesar de las

dificultades; a mis hermanos y hermanas, quienes me ayudaron y dieron aliento para continuar con mis estudios. A los catedráticos de la Facultad de Ciencias Económicas de la prestigiosa Universidad de El Salvador, quienes compartieron sus conocimientos para formarme profesionalmente. Finalmente, y no menos importante, agradezco a mis compañeros y amigos, con quienes intercambiamos opiniones para formar criterios.

***Noé Aquiles Rivera Carrillo.***

Agradezco a Dios, por guiar mis pasos con sabiduría, darme fortaleza en momentos de flaqueza. A mi madre Beatriz Berciano por todo su amor, comprensión, sacrificio y apoyo incondicional, a mis hermanas por estar siempre a mi lado apoyándome y aconsejándome, a todos mis amigos y familiares que durante mi proceso de preparación académica compartieron y transmitieron sus conocimientos; a mis compañeros de trabajo por mantenerse perseverantes durante el proceso de especialización; a los docentes y asesores que nos ofrecieron su tiempo y conocimiento en el desarrollo del trabajo.

***Metzi Danelia Vásquez Berciano.***

# ÍNDICE

## ÍNDICE DE TABLAS

**CONTENIDO** **PÁG NO.**



## ÍNDICE DE FIGURAS

**CONTENIDO** **PÁG NO.**

# RESUMEN EJECUTIVO

En la actualidad, los avances tecnológicos permiten realizar procesos mecanizados y sistematizados con mucha más eficacia y eficiencia, lo que resulta de gran utilidad a todos los profesionales en auditoría forense, pues mediante el apoyo de diferentes herramientas se reducen los tiempos para la ejecución de los encargos y generan una mayor fiabilidad de la información a analizar, así como el resguardo de esta. Pero para que sean aprovechadas todas las ventajas que estas tecnologías ofrecen es necesario que el auditor tenga pleno conocimiento de su funcionamiento, por tal motivo esta investigación describe el uso de las tecnologías RegTech y SupTech en las auditorías forenses con enfoque preventivo, a fin de aprovechar su uso en los encargos aplicados a empresas FinTech que operan en el área metropolitana de San Salvador.

Para entender el uso de estas tecnologías es necesario describir los procesos realizados por este tipo de herramientas de supervisión y regulación tecnológicas, que utilizan las empresas FinTech y con ello establecer las ventajas que brindan en la realización de auditorías forenses con enfoque preventivo e identificar los riesgos asociados a estas tecnologías.

La presente investigación es de tipo hipotético-deductivo, pues se parte de una hipótesis no comprobable de forma directa. La naturaleza es cualitativa, por lo que se hace uso de la técnica de sistematización bibliográfica y de entrevistas aplicadas a auditores con experiencia en encargos de aseguramiento y con conocimiento sobre el funcionamiento de las FinTech y a miembros de la Asociación Salvadoreña de Tecnología

Financiera, quienes comentaron sobre la importancia y los beneficios de apoyarse en estas herramientas para validar la eficacia de los controles que implementan para la prevención y detección de posibles fraudes.

Dentro de los resultados de la investigación, cabe resaltar la importancia que el auditor forense tenga la experiencia en la ejecución de auditoría de sistemas o se apoye con un profesional que certifique los procesos realizados por las SupTech y las RegTech de tal manera que, al utilizar los lineamientos propuestos en el presente trabajo, pueda plantear programas de auditoría encaminados a verificar el cumplimiento de las leyes y normativas emitidas en materia de prevención de fraude y de supervisión basada en riesgos.

Por lo tanto, se concluye que actualmente en nuestro país se desconocen los beneficios del uso las herramientas tecnológicas de supervisión y regulación aplicadas a los encargos forenses con enfoque preventivo; sin embargo, de forma implícita muchas entidades y plataformas aplican las diferentes RegTech para el procesamiento, extracción y recopilación de información. Es necesario que los licenciados en contaduría pública se capaciten en el uso y aplicación de las nuevas herramientas tecnológicas que ayudan a la ejecución de encargos forenses. Además, es de tener en cuenta que los procedimientos que se ejecuten en este tipo de encargos, deben apoyarse en las herramientas RegTech y SupTech, pues son las que se encargan de dar cumplimiento a los requisitos legales y normativos por medio de la automatización de procesos y monitoreo de operaciones que permiten prevenir, detectar y reportar los riesgos de blanqueo de capital; por lo tanto, es de vital importancia que el auditor posea la experticia necesaria para validar que los reportes generados por estas tecnologías son adecuados.

# INTRODUCCIÓN

La utilización de tecnologías como apoyo para la ejecución de auditorías forenses, se ha visto en la necesidad de adaptar los procedimientos para la extracción, procesamiento y análisis de la información, por lo que el profesional acreditado para realizar trabajos forenses debe estar a la vanguardia de las actualizaciones tecnológicas y saber aprovechar los recursos que se ponen a su disposición. Por tal motivo es importante llevar acabo esta investigación que tiene como propósito describir el uso de las tecnologías RegTech y SupTech en la auditoría forense con enfoque preventivo, a fin de aprovechar su uso en los encargos aplicados a empresas FinTech que operan en el área metropolitana de San Salvador.

La investigación está dividida en tres capítulos:

En el primer capítulo, se incluye el planteamiento del problema, en el que se plasma la problemática identificada en forma de pregunta, la delimitación de la investigación, se justifica la importancia de su realización y se plantean los objetivos que se persiguen con la misma. Además, se incluye el marco teórico en el que se describen los antecedentes del problema, se aclaran algunos conceptos que son fundamentales para la comprensión de la materia sujeta de estudio y se incluyen las normativas y bases legales que soportan la investigación.

El segundo capítulo, contiene el diseño metodológico que describe los instrumentos que se utilizaron para la obtención de información de las unidades sujetas de análisis; además de explicar la forma en cómo fue procesada la información recolectada

y se incluyen los lineamientos que son clave para el planteamiento de los programas de auditoría.

En lo que respecta al tercer capítulo, se proponen programas de auditoría forenses con enfoque preventivo aplicados a empresas FinTech que operan en el área metropolitana de San Salvador apoyados en la utilización de las tecnologías SupTech y RegTech.

Finalmente, el presente documento contiene sus respectivas conclusiones y recomendaciones, así como los anexos de las entrevistas realizadas a expertos.

# CAPÍTULO I- PLANTEAMIENTO DEL PROBLEMA

## 1.1 Situación problemática de la utilización de las tecnologías SupTech y RegTech en las auditorías forenses con enfoque preventivo aplicadas a empresas FinTech que operan en el área Metropolitana de San Salvador

La llegada de la inteligencia artificial ha sido aprovechada por el sistema financiero para mejorar, automatizar y masificar los procesos que permiten el registro y supervisión de las transacciones bancarias. El sistema bancario tradicional ha tenido que adaptarse a las exigencias de una sociedad altamente digitalizada, teniendo que invertir en la adquisición de plataformas y aplicativos que ayuden a promocionar, facilitar y aprovechar los productos ofrecidos por estas instituciones.

Sin embargo, los esfuerzos de la banca por adaptarse a un entorno tecnológico cambiante, han sido opacados por el auge de las FinTech, que no solo utilizan la tecnología para prestar los servicios financieros tradicionales; sino que, son capaces de adaptarse a nuevos modelos de negocio.

Los acontecimientos que han dado paso a la creación de las empresas FinTech datan del año 1950 con el aparecimiento de las tarjetas de crédito y débito, que contribuyeron al mejoramiento de la portabilidad del dinero. De 1960 a 1970, se crea la posibilidad de hacer retiros de efectivo sin la restricción de horarios que ponían las entidades bancarias gracias a la entrada de los cajeros automáticos; además, se crean los primeros medios para la compra y venta de acciones en las diferentes bolsas de valores a nivel mundial.

De 1780 al 2000, la revolución tecnológica permite el aparecimiento de computadoras, celulares y el uso de internet, lo que sirve de base para introducir el comercio electrónico. A partir del 2010, la consolidación de la banca digital impulsa la disposición de plataformas y aplicativos móviles que permiten la disposición de servicios financieros, sin dejar de lado la llegada de las pasarelas de pago.

Como resultado de la combinación entre banca tradicional y la utilización de tecnologías, nace un nuevo modelo de operar en el entorno financiero llamado FinTech, que no solo se ocupa de brindar los servicios ofrecidos por los bancos, sino que, permite la inclusión de más servicios y productos financieros.

Con la introducción de este nuevo ecosistema financiero, surgen las tecnologías de regulación (RegTech) y de supervisión (SupTech), por lo que en un principio se les conoció como un subconjunto de las FinTech; aunque, debido a su amplia capacidad de adaptación y necesidad de su uso, su campo de aplicación se ha diversificado. Su importancia en las FinTech radica en la optimización de recursos y la obtención de informes a la medida, por lo que, las ventajas de su uso generan beneficio a las empresas que las utilizan.

Los auditores deben estar en la vanguardia de la actualización para comprender la forma de operar de estas empresas y conocer los posibles riesgos de fraude a los que podría enfrentarse, pues esta nueva estructura financiera, aunque aumente la automatización y procesamiento de información, trae consigo un factor de riesgo asociado a la variedad y volumen de transacciones que realiza. Por lo tanto, las bases de datos que se ponen a disposición del auditor forense necesitan ser evaluados de forma rigurosa para lograr identificar posibles anomalías o alertas sobre las cuales centrar su investigación.

Por lo mencionado anteriormente, es de gran utilidad para los auditores apoyarse en las RegTech, que buscan adaptar las normativas vigentes a nuevos sistemas de negocio a fin de dar soluciones regulatorias eficientes y de SupTech que ejecuta supervisiones con la finalidad de garantizar que las entidades FinTech no tengan inconvenientes de cumplimiento legal.

## 1.2 Enunciado del problema

La utilización de las herramientas SupTech y RegTech contribuyen a la transparencia de las operaciones de las entidades FinTech, por lo que el auditor debe conocer el funcionamiento de estas para tener claridad de las áreas o puntos que le servirán para realizar un encargo de auditoría forense; por lo que la investigación va orientada a la siguiente problemática:

¿En qué medida incide la no utilización de las tecnologías SupTech y RegTech en las auditorías forenses con enfoque preventivo aplicadas a empresas FinTech que operan en el área metropolitana de San Salvador?

## 1.3 Justificación de la investigación

### 1.3.1 Novedoso

Es novedoso el desarrollo de la investigación, ya que actualmente los panoramas financieros se están innovando con el uso de la tecnología, ocasionando que las empresas FinTech requieran mayor capacidad de supervisión y regulación para asumir las oportunidades, riesgos y desafíos que los cambios tecnológicos puedan generar.

La constante actualización o innovación tecnológica debe proporcionar un grado de seguridad razonable, contribuyendo así, a la aplicación de tecnologías adecuadas para la supervisión y regulación de operaciones financieras a través de herramientas como la SupTech que ayuda a agilizar los procesos de supervisión, vigilancia, análisis de informes y generar indicadores de riesgo en tiempo real para respaldar la supervisión prospectiva basada en juicios y formulación de políticas; mientras que la RegTech eficientiza la capacidad de gestión de riesgos y produce nuevos conocimientos sobre el negocio para la toma de decisiones.

### 1.3.2 Utilidad social

La explicación del uso de las herramientas SupTech y RegTech beneficia a los profesionales permitiendo la optimización de extracción de información y agilizando procesos analíticos que sirvan de base para el desarrollo de trabajos de auditoría forense.

### 1.3.3 Factibilidad

- ✓ Bibliográfica

Se utilizaron diversas fuentes bibliográficas entre ellas revistas, documentos, sitios web confiables, reseñas, trabajos de investigación, boletines y videos que abordan la temática de estudio, que ayudaron al desarrollo de la investigación y permitieron exponer de manera teórica, técnica y legal la problemática planteada.

- ✓ De campo

Se tuvo acceso a información por parte de profesionales capacitados en el uso y aplicación de las herramientas SupTech y RegTech, para que permita comprender su funcionamiento y aplicación en empresas FinTech. Además, se contó con el apoyo de asesores que proporcionaron sugerencias de bibliografía y redacción del documento.

## 1.4 Objetivos

### 1.4.1 Objetivo general

Describir el uso de las tecnologías RegTech y SupTech en las auditorías forenses con enfoque preventivo, a fin de aprovechar su uso en los encargos aplicados a empresas FinTech que operan en el área metropolitana de San Salvador.

### 1.4.2 Objetivos específicos

- Describir los procesos realizados por las tecnologías SupTech y RegTech utilizados por las empresas FinTech, a fin de tener una mejor comprensión de su funcionamiento y los tipos de informes que brindan.

- Establecer las ventajas del uso de las tecnologías RegTech y SupTech en la realización de auditorías forenses con enfoque preventivo, para determinar su importancia.

- Identificar los riesgos asociados a las tecnologías RegTech y SupTech, de tal manera que puedan proponerse programas de auditoría que sirvan de base para la identificación de deficiencias en los procesos que contribuyen a la prevención de fraudes.

## 1.5 Principales definiciones

- **FinTech**

Empresa de nueva creación que comercializa productos y/o servicios a través del uso intensivo de las tecnologías de la información y la comunicación (TIC's), con un modelo de negocio escalable el cual le permite un crecimiento rápido y sostenido en el tiempo (López, 2018).

- **Startup**

Un startup es una pequeña empresa de reciente creación, con alto potencial innovador y tecnológico, donde su modelo es escalable y su crecimiento puede ser exponencial. El término start-up significa "puesta en marcha". Y, efectivamente, podemos definirlo como el periodo inicial de una empresa, el comienzo o arranque de un nuevo negocio. (Cuellar, 2015).

- **SupTech**

Su nombre proviene de Supervisory Technology (tecnología de supervisión) y se refiere a la aplicación de tecnologías RegTech en los órganos supervisores. Es decir, mientras que las RegTech se dedican a ayudar a los bancos a cumplir con regulaciones usando diversas tecnologías, las SupTech agilizan y automatizan procesos al interior de las instancias reguladoras; son la contraparte de las RegTech.

- **RegTech**

Considerada como una subcategoría de las FinTech y proveniente de la frase en inglés Regulatory Technology (tecnología regulatoria). Se trata de servicios dedicados a facilitar y supervisar el cumplimiento de requerimientos regulatorios. A través de tecnologías como la nube, blockchain o el big data, estas compañías ayudan a ahorrar tiempo y esfuerzo a la hora de dicho cumplimiento (MAAT.AI, 2020).

- **Auditoría forense**

Es la técnica de investigación criminalística, integradas con la contabilidad, conocimientos jurídico-procesales, y con habilidades en finanzas y de negocio, para manifestar información y opiniones, como pruebas en los tribunales. El análisis resultante además de poder usarse en los tribunales, puede servir para resolver las disputas de diversas índoles, sin llegar a sede jurisdiccional (C.V, s.f.).

- **Auditoría forense preventiva**

Orientada a proporcionar aseguramiento (evaluación) o asesoría a las organizaciones respecto a su capacidad para disuadir, prevenir (evitar), detectar y reaccionar ante fraudes financieros, puede incluir trabajos de consultoría para implementar: programas y controles antifraude, esquemas de alerta temprana de irregularidades y sistemas de administración de denuncias. Este enfoque es proactivo por cuanto implica tomar decisiones y acciones en el presente, para evitar fraudes en el futuro (Haddad, 2011).

- **Blockchain.**

  Se puede definir como una estructura matemática para almacenar datos de una manera que es casi imposible de falsificar. Es un libro electrónico público que se puede compartir abiertamente entre usuarios dispares y que crea un registro inmutable de sus transacciones.

## 1.6 Generalidades

### Diferencia de las entre las herramientas tecnológicas de regulación y supervisión

RegTech es la herramienta que centra su aplicación en el ámbito del cumplimiento normativo y SupTech es la aplicación de controles de supervisión en las diferentes áreas de riesgos de una entidad.

### Funciones

- Brindar seguridad en la aplicación de marcos regulatorios a los nuevos modelos de comercio.

- Optimizar el proceso de recopilación de datos y generación de informes.

- Monitorear el debido cumplimiento de las políticas y procedimientos administrativos.

- Ayudar en la identificación y gestión de las principales áreas de riesgos.

- Proporcionar soluciones mediante la aplicación de cumplimiento normativos.

- Desarrollo de programas preventivos de supervisión.

- Aplicación de controles en el proceso de ingreso y extracción de información.

- Permiten gestionar el riesgo mediante una supervisión dinámica y predictiva.

La tecnología RegTech involucra los procesos regulatorios principalmente en tareas económicas con implicación compleja de regulaciones, la SupTech centra su aplicación en tecnologías que optimizan los procedimientos de extracción de información.

**1.7 Base técnica**

- Norma Internacional De Encargos De Aseguramiento 3000 (NIEA 3000)

Dentro de sus objetivos se encuentra "expresar una conclusión sobre el resultado de la medición o evaluación de la materia subyacente objeto de análisis, ya sea mediante un informe escrito con una conclusión de seguridad razonable o de seguridad limitada y que describe la base de la conclusión" (IFAC, 2016)

- Estándares Internacionales Sobre La Lucha Contra El Lavado De Activos Y El Financiamiento Al Terrorismo Y La Proliferación

De las 40 recomendaciones del GAFI, para efectos de la investigación se retomarán las siguientes:

**R.5 Debida diligencia del cliente.**

De acuerdo con esta recomendación, no se deben mantener cuentas anónimas o cuentas con nombres ficticios; además se deben implementar medidas de Debida Diligencia del cliente (DDC) como las siguientes:

a) Identificar al cliente y verificar la identidad del cliente utilizando los documentos, datos o información confiable de fuentes independientes.

b) Identificar al beneficiario final y tomar medidas razonables para verificar la identidad del beneficiario final, de manera tal que la institución financiera esté convencida de que conoce quién es el beneficiario final. Para las personas jurídicas y otras estructuras jurídicas, esto debe incluir que las instituciones financieras entiendan la estructura de titularidad y de control del cliente.

c) Entender y cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial.

d) Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esta relación para asegurar que las transacciones que se realicen sean consistentes con el conocimiento que tiene la institución sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

En el caso de que no se pueda dar cumplimiento a los requisitos aplicables de los literales antes citados, la institución no puede abrir la cuenta del cliente.

**R.10 Mantenimiento de registros.**

Se recomienda que las instituciones mantengan los registros necesarios y suficientes sobre todas las transacciones por al menos 5 años, de tal manera que pueda ser proporcionada a las autoridades competentes cuando éstas así lo requieran para ser utilizadas como evidencia para el enjuiciamiento de una actividad criminal.

Esta información incluye los datos recogidos mediante las medidas de Debida Diligencia del Cliente como, por ejemplo: copias o registros de documentos oficiales de identificación como pasaportes, tarjetas de identificación, licencias de conducción o documentos similares, expedientes de cuentas y correspondencia comercial, incluyendo los resultados de los análisis que se hayan realizado.

**R.14 Revelación (tipping-off) y confidencialidad.**

Las instituciones financieras, sus directores, funcionarios y empleados deben:

a) Estar protegidos por la ley frente a la responsabilidad penal y civil por violación de alguna restricción sobre la revelación de la información impuesta mediante contrato o mediante alguna disposición legislativa, normativa o administrativa, si éstos reportan sus sospechas de buena fe a la UIF, aun cuando no conocieren precisamente cuál era la actividad criminal subyacente, e independientemente de si la actividad ilegal realmente ocurrió o no; y

b) Tener prohibido por la ley revelar (“tipping-off”) el hecho de que se está entregando a la UIF un reporte de operaciones sospechosa (ROS) o información relacionada.

**R.23 Regulación y supervisión de instituciones financieras.**

Según esta guía son los diferentes países los que deben asegurar que las instituciones financieras estén sujetas a regulaciones y supervisión adecuadas, además de que se implementen las Recomendaciones de GAFI.

**R.29 Facultades de los supervisores.**

Establece que los entes supervisores deben tener la facultad de supervisar y monitorear las instituciones financieras con el fin de asegurar que se cumplan con los lineamientos para combatir el lavado de activos y el financiamiento al terrorismo.

Dentro de las facultades y potestades con las que deben contar los supervisores están: Imposición de una gama de sanciones disciplinarias y financieras, además de la potestad para retirar, restringir o suspender la licencia de la institución financiera.

- Normas Técnicas Para La Gestión De Los Riesgos De Lavado De Dinero Y De Activos Y Financiamiento Al Terrorismo

Según el Art. 1, “el objeto de estas Normas es proporcionar los lineamientos mínimos para la adecuada gestión del riesgo de lavado de dinero y de activos y de financiamiento al terrorismo, a fin de que las entidades integrantes del sistema financiero prevengan y detecten operaciones irregulares o sospechosas relacionadas con el referido riesgo, de forma oportuna” (Comité De Normas Del Banco Central De Reserva De El Salvador, 2013) .

- NTS ISO/IEC 27001:2013

Norma que contiene los requerimientos para establecer, implementar, mantener y mejorar continuamente los sistemas que permiten la gestión de seguridad de información enmarcado en el contexto de la organización.

## 1.8 Base legal

- Ley Para Facilitar La Inclusión Financiera

Esta ley fomenta la competencia en el sistema financiero y permite la reducción de costos para los usuarios y los clientes, regulando aspectos importantes como el dinero electrónico, la protección de datos y prohibiciones para los proveedores de dinero electrónico.

- Ley Para Facilitar El Acceso Al Crédito

Permite la competitividad de las empresas FinTech al permitirles otorgar créditos pequeños a clientes que deben cumplir con requisitos menos rigurosos que los exigidos por la banca tradicional.

- Ley de Firma Electrónica y su Reglamento

Su aplicabilidad va dirigida a la comunidad electrónica, firma electrónica certificada y firma electrónica simple; incluyendo los desarrollos tecnológicos que se produzcan en el futuro.

# CAPÍTULO II- METODOLOGÍA DE LA INVESTIGACIÓN

## 2.1 Enfoque y tipo de investigación

El tipo de estudio que se realizó es hipotético-deductivo por lo que se partió de una hipótesis no comprobable directamente, tomando de base un enunciado general y a partir del cual se pretendió dar una propuesta de solución mediante estudios bibliográficos, utilizando instrumentos de recolección de datos y observaciones.

La investigación desarrollada es de naturaleza cualitativa, por lo que se requirió el estudio de la problemática desde la perspectiva de las partes directamente involucradas; es decir, describiendo el uso de las tecnologías SupTech y RegTech en la realización de auditorías forenses aplicadas a empresas FinTech que operan en el área metropolitana de San Salvador.

## 2.2 Delimitación de la investigación

### 2.2.1 Teórica

La investigación se desarrolló bajo la perspectiva de una auditoría forense con enfoque preventivo, a fin de sustentar en normativa técnica local e internacional, estándares internacionales, leyes vigentes en El Salvador y otras regulaciones que sean necesarias para respaldar la investigación.

Se utilizaron como fuente de información las siguientes:

- Norma Internacional De Encargos De Aseguramiento 3000. (NIEA 3000).

- Estándares Internacionales Sobre La Lucha Contra El Lavado De Activos Y El Financiamiento Al Terrorismo Y La Proliferación (Recomendaciones del GAFI), para efectos de la investigación se retomarán las siguientes:
  - ✓ Recomendación N°5 “Debida diligencia del cliente”.
  - ✓ Recomendación N°10 “Mantenimiento de registros”.
  - ✓ Recomendación N°14 “Revelación (tipping-off) y confidencialidad”.
  - ✓ Recomendación N°23 “Regulación y supervisión de instituciones financieras”.
  - ✓ Recomendación N°24 “Regulación y supervisión de las APNFD”.
  - ✓ Recomendación N°29 “Facultades de los supervisores”.
- Normas Técnicas Para La Gestión De Los Riesgos De Lavado De Dinero Y De Activos Y Financiamiento Al Terrorismo.
- ISO 27001 - Software ISO 27001 de Sistemas de Gestión
- Ley Para Facilitar La Inclusión Financiera.
- Ley Para Facilitar El Acceso Al Crédito
- Ley de Firma Electrónica y su Reglamento.

### 2.2.2 Temporal

Con la finalidad de entender cómo los avances en la tecnología ayudan al auditor forense a realizar sus procedimientos para prevenir posibles fraudes, la presente investigación se centra en la información recabada entre los años 2015 y 2021.

### 2.2.3 Geográfica

El límite espacial de la investigación está centrado en las empresas FinTech que tienen operaciones en el área metropolitana de San Salvador, departamento de San Salvador.

## 2.3 Sujetos y objetos de estudio

### 2.3.1 Unidad de análisis

La realización de la investigación se hizo con la colaboración de:

- Auditores con experiencia en auditoría de encargos de aseguramiento y con conocimiento sobre el funcionamiento de las FinTech.
- Representante de la Asociación de Tecnología Financiera de El Salvador (ASAFINTECH).

### 2.3.2 Variables e indicadores

Variable independiente:

La utilización de las tecnologías SupTech y RegTech en las auditorías forenses.

Variable dependiente:

Facilitar las auditorías forenses con enfoque preventivo aplicadas a empresas FinTech que operan en el área metropolitana de San Salvador.

Ver operacionalización de variables en tabla 1

**Tabla 1**

*Operacionalización de Variables*

| Formulación del Problema | Objetivo General | Hipótesis del trabajo | Elementos de la Hipótesis | Variable | Indicadores | Instrumentos |
|---|---|---|---|---|---|---|
| ¿En qué medida incide la no utilización de las tecnologías SupTech y RegTech en las auditorías forenses con enfoque preventivo aplicadas a empresas FinTech que operan en el área metropolitana de San Salvador? | Describir el uso de las tecnologías RegTech y SupTech en las auditorías forenses con enfoque preventivo, a fin de aprovechar su uso en los encargos aplicados a empresas FinTech que operan en el área metropolitana de San Salvador | La utilización de las tecnologías SupTech y RegTech en las auditorías forenses, son útiles para facilitar los encargos con enfoque preventivo en las empresas FinTech que operan en el área metropolitana de San Salvador. | Tener el conocimiento teórico y práctico para la utilización de las tecnologías SupTech y RegTech en las auditorías forenses. | **Independiente:** La utilización de las tecnologías SupTech y RegTech en las auditorías forenses. | (a) Análisis de los informes que proveen las tecnologías SupTech y RegTech<br>(b) Verificación de los requerimientos normativos y legales. | **Entrevistas:** Se utilizaron como medio para obtener información por medio del diálogo directo con profesionales en el desarrollo de auditorías que posean experiencia en encargos de aseguramiento y con conocimiento sobre la forma de operar de las empresas FinTech<br>**Ficha Bibliográfica:** La recolección de documentación permitió la extracción de literatura que contribuyó a la redacción de ideas concretas que facilitaron la comprensión del tema investigado |
| | | | Tener el conocimiento del enfoque preventivo en las auditorías forenses aplicables a las empresas FinTech, con el fin de establecer procesos de auditoría que ayuden al aprovechamiento de las tecnologías en la realización de encargos de aseguramiento. | **Dependiente:** Facilitar los encargos con enfoque preventivo en las empresas FinTech que operan en el área metropolitana de San Salvador. | (a) Descripción de las operaciones realizadas por empresas FinTech en El Salvador.<br>(b) Aplicación de los requerimientos de la Norma Internacional de Encargos de Aseguramiento. | **Parámetros de medición**<br>* Facilita la obtención de evidencia sobre la calidad de los controles preventivos de fraude.<br>* Contribuye a la adaptación de regulaciones futuras. |

## 2.4 Técnicas e instrumentos utilizados

Para el desarrollo de la investigación, se hizo uso de las técnicas e instrumentos siguientes:

### Técnicas

- Entrevistas.

  Se utilizó como medio para obtener información, el diálogo directo con profesionales en el desarrollo de auditorías que poseen experiencia en encargos de aseguramiento y con conocimiento sobre la forma de operar de las empresas FinTech.

- Sistematización Bibliográfica

  Se consultó el material bibliográfico necesario para la comprensión y posterior sistematización de ideas que contribuyeron a la resolución de la problemática abordada.

### Instrumentos

- Guía de preguntas para entrevistas.

  Se redactó una serie de preguntas que fueron autorizadas por el asesor especialista, con las cuales se obtuvo información clave para argumentar la propuesta de solución.

- Ficha bibliográfica.

La recolección de documentación permitió la extracción de literatura que contribuyó a la redacción de ideas concretas que facilitaron la comprensión del tema investigado.

## 2.5 Procesamiento y análisis de la información

### 2.5.1 Procesamiento de la información

Las entrevistas que se realizaron a los expertos en el tema fueron grabadas mediante la plataforma Meet, de tal manera que sus respuestas pudieron ser consultadas para ser tabuladas mediante el programa de Microsoft Word, lo que facilitó la elaboración de tablas que permitieron un mayor análisis de las respuestas obtenidas. En lo que respecta a la información bibliográfica, se mantuvo una carpeta en Drive con la documentación utilizada para fundamentar el contenido del trabajo.

Se depuró la información bibliográfica recolectada, dejando solo información documental adecuada; a la que se le dio lectura comprensiva para adquirir conocimiento y mediante la sistematización de la información, se presentaron ideas resumidas que contienen información relativa a la fuente original.

### 2.5.2 Análisis de la información

Se procedió a analizar cada una de las respuestas obtenidas en la entrevista realizada al representante de la Asociación de Tecnología Financiera de El Salvador y el auditor con experiencia en encargos de aseguramiento y con conocimientos sobre el funcionamiento de empresas FinTech. Las respuestas a la entrevista y el respectivo análisis se describen en la presentación de resultados mediante el uso de tablas y

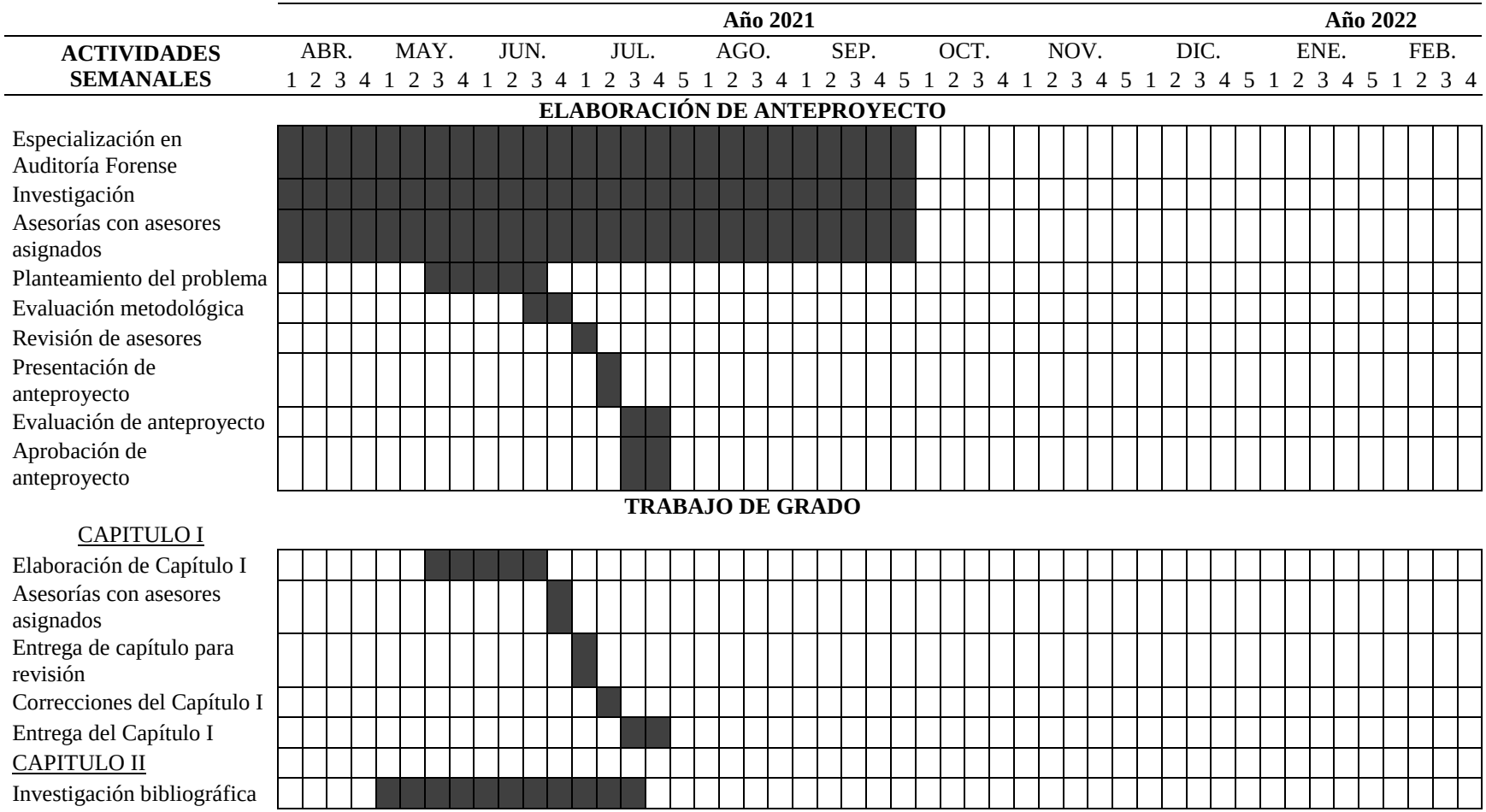
posteriormente se muestra el diagnóstico planteado en función de las respuestas obtenidas.

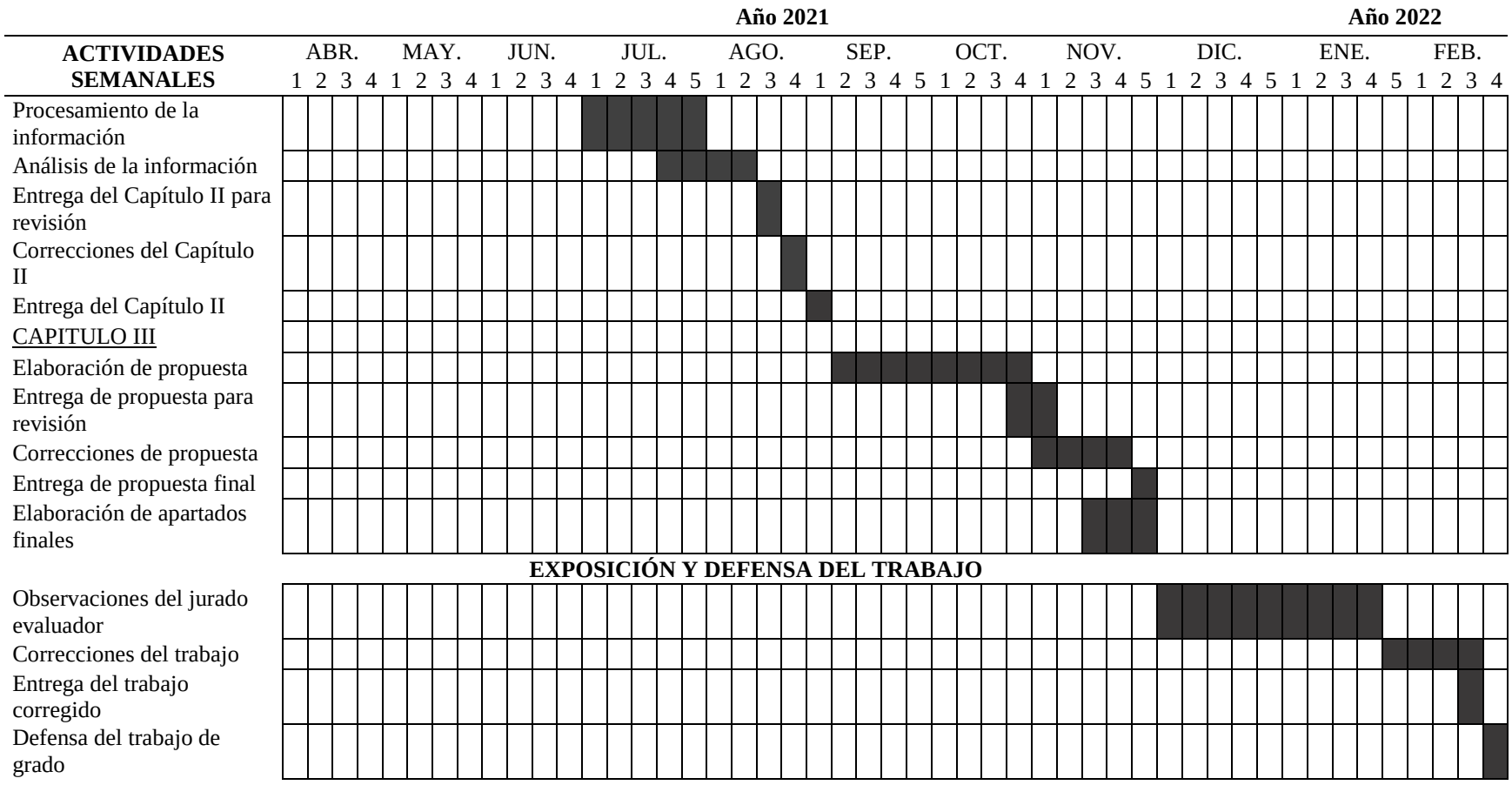
## 2.6 Cronograma de actividades

La programación de las actividades a desarrollar para la realización de la investigación se detalla en el cronograma de actividades. Ver tabla 2

**Tabla 2**

*Cronograma de actividades*




Año 2021
Año 2022
ACTIVIDADES SEMANALES
ABR. MAY. JUN. JUL. AGO. SEP. OCT. NOV. DIC. ENE. FEB.
1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 5 1 2 3 4 1 2 3 4 5 1 2 3 4 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4
Procesamiento de la información
Análisis de la información
Entrega del Capítulo II para revisión
Correcciones del Capítulo II
Entrega del Capítulo II
CAPITULO III
Elaboración de propuesta
Entrega de propuesta para revisión
Correcciones de propuesta
Entrega de propuesta final
Elaboración de apartados finales
EXPOSICIÓN Y DEFENSA DEL TRABAJO
Observaciones del jurado evaluador
Correcciones del trabajo
Entrega del trabajo corregido
Defensa del trabajo de grado

## 2.7 Presentación y análisis de los resultados

La presentación de las respuestas obtenidas de las entrevistas realizadas al representante de la Asociación de Tecnología Financiera de El Salvador y al profesional con experiencia en la realización de encargos de aseguramiento con conocimientos sobre el funcionamiento de empresas FinTech se realiza mediante tablas, en las cuales se detalla la pregunta realizada, un extracto de la respuesta que se obtuvo y el respectivo análisis de esa respuesta. Ver tabla 3 y 4.

**Tabla 3**

*Resultados de la entrevista al representante de la Asociación de Tecnología Financiera de El Salvador (ASAFINTECH)*

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 1 | ¿Qué es FinTech y cómo funcionan? | FinTech es la unión de Finance y Tecnology. Nacen en San Francisco California, en Sillicon Valey es donde nace este tipo de tecnologías llamadas Startups, crecieron muchísimo en las últimas décadas con un modelo de negocio bastante agresivo, en donde estas empresas desarrollan servicios basados en tecnología y tienen un ciclo de crecimiento más rápido que las empresas tradicionales, se les inyecta mucho capital, utilizan mucha tecnología, la adopción de los clientes es mucho más rápido que una empresa tradicional y este fue un movimiento que sucedió principalmente después de las punto com o incluso junto con las punto com en el área de Sillicon Valey. La Universidad de Stanford ha empujado muchísimo la creación del ecosistema de Startups. Como estas empresas demandan mucho capital para su crecimiento acelerado, hay muchos inversionistas a los que se les llama inversionista de capital de riesgo y estos fondos de inversión son los que fondean estas empresas, entre ellas aplicaciones que desarrollan soluciones de tecnologías en agricultura, logística, para el mundo de finanzas, salud, etc. Pero en los años se observó que las categorías que se volvían más atractivas para los fondos de inversión eran las empresas de tecnología financiera y por eso ellos | El término FinTech puede definirse como servicios financieros innovadores impulsados por los inversionistas de capital de riesgo y su característica principal es que su funcionamiento está basado en la aplicación de tecnología.<br>Dentro de este tipo de soluciones financieras se encuentran diferentes categorías, a las que se les conoce como verticales.<br>La vertical principal es la de pago cuyos servicios incluyen pagos con tarjetas e inclusive el bitcoin, billeteras electrónicas, remesas internacionales, pagos de facturas, entre otros. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | acuñaron el tema FinTech que son aplicaciones o Startups o empresas basadas en tecnología, pero orientado al mundo de las transacciones financieras.<br>Dentro del mundo FinTech hay categorías o verticales. Las principales son las verticales de pagos, es decir, ahí se agrupan todas las empresas FinTech que desarrollan soluciones alrededor de pagos y ahí incluye pagos con tarjetas e inclusive el bitcoin, billeteras electrónicas, remesas internacionales, pagos de facturas, etc.<br>La otra vertical más grande es la vertical de créditos digitales o innovación de créditos. Hay otro montón de empresas que se dedican principalmente en muchas formas distintas a otorgar créditos a consumidores o créditos para empresas. | |
| 2 | ¿Considera necesario la creación de una Ley FinTech? ¿Por qué? | No existe una ley. Hoy por hoy sabemos que el Banco Central con apoyo del Banco Mundial están trabajando en la creación de una ley FinTech. Como asociación creemos que la ley FinTech puede jugar a favor o en contra del gremio si no se analiza y discute adecuadamente. La ley FinTech tiene puntos a favor, principalmente hace un marco donde los inversionistas lo ven positivamente porque si hay reglas claras y hay una cancha ya marcada; es decir, si no hay reglas claras, la inversión que se atrae es poca. Entonces con una ley podemos atraer inversión extranjera para las empresas FinTech. Por otro lado, sabemos que las verticales de FinTech son variables y | La creación de una ley FinTech que no sea bien planteada puede traer limitantes para el crecimiento de este ecosistema, pues si las regulaciones que se imponen son demasiado estrictas, sería necesario que para su entrada en el mercado se tenga que contar con capitales que los pequeños inversionistas difícilmente alcanzarían.<br>Por otra parte, la inexistencia de una Ley FinTech no implica una limitante para poder operar en el país, pues existen regulaciones ya establecidas en el ámbito financiero que este tipo de empresas deben cumplir y que les |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | una ley FinTech no abarca todas las verticales, entonces, decir que tenemos una ley FinTech universal es mentira. Ni el caso de México del que hablan mucho y que es una ley super buena no cubre todas las verticales, solo cubre un par. En Estados Unidos existe la figura de la empresa de servicios bancarios complementarios, entonces cuando surge una FinTech entra dentro de esa regulación, dentro de la figura de empresa de servicios complementarios y eso nos gusta mucho más porque deja abierta la creatividad y no cierra la puerta. Otra de las cosas en contra de la Ley FinTech como es el caso de México que crean una cosa que se llama Sandbox que hace que las empresas o las FinTech entren a un grupo de empresas supervisadas por un ente regulador, pero deja fuera un montón porque los requisitos para entrar son muy altos; eso estrangula la creatividad y los pequeños no tienen oportunidad de competir, entonces entran FinTech que son financiadas por los bancos, por aseguradoras o por grupos grandes y al pequeño no lo dejan competir; entonces eso nos parece malísimo de la ley. | permite ser más competitivas en el sector, sin pasar por alto los requisitos de legalidad de sus operaciones. |
| 3 | ¿Poseen las FinTech oficiales de cumplimiento? | Depende de en qué regulación caiga la empresa FinTech. Hoy por hoy, como no hay una regulación universal, cada empresa hace su propia evaluación, su propio assessment y lo que hacen es autorregularse. Algunas pueden invertir en un oficial de cumplimiento, otros tratan de evitar este gasto porque | Debe analizarse la jurisprudencia aplicable a la FinTech en función de la vertical en la que se clasifique, pues dependerá de la ley y de su capital la obligación de contratar o no a un oficial de cumplimiento. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | son empresas jóvenes con limitaciones grandes de capital para contratar mucho personal. Por ejemplo, una FinTech que está en la vertical de remesas, posiblemente la ley lo obligue a tener un oficial de cumplimiento. Entonces depende de en qué regulación caiga o en qué vertical esté la FinTech puede tener un oficial de cumplimiento o no puede tenerlo. | |
| 4 | ¿Considera usted que la implementación de SupTech y RegTech pueden llegar a reemplazar a los oficiales de cumplimiento? | No creo, todas esas son herramientas que ayudan a tomar decisiones más rápidas o automatizar procesos manuales, pero no eliminan la necesidad de tener una persona que tome decisiones en ese aspecto y supervisando, porque al final el oficial de cumplimiento es un papel de autosupervisión, estar viendo que los procesos internos estén sucediendo adecuadamente o acorde a lo que la ley establece y una computadora, una tecnología puede automatizar procesos pero no necesariamente va a sustituir ese rol. | Estas herramientas no sustituyen la necesidad de nombrar un oficial de cumplimiento, pues las funciones que éste desempeña van encaminadas a la toma de decisiones, por lo que las SupTech y RegTech vienen a faciliar los procedimientos y la información para que las decisiones que se tomen sean más adecuadas. |
| 5 | ¿Conoce usted sobre casos de fraudes que se hayan detectado en el ecosistema FinTech en El Salvador? | No y eso es algo muy importante de mencionar porque muchas veces se atacan a las FinTech por ser empresas que no tienen suficiente control, supervisión, etc. pero los que supuestamente tienen toda la tecnología y toda la supervisión están permitiendo que a la gente se les robe el dinero y nadie les dice nada. | Aunque las FinTech no cuenten con una Ley específica, el marco legal aplicable y la ayuda de la tecnología permite eficientizar sus controles para evitar fraudes. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 6 | ¿Qué es RegTech y cómo funcionan? | RegTech es tecnología regulatoria que ayuda a empresas que desarrollan soluciones para ayudar a la parte de cumplimiento, por ejemplo, la RegTech que se tiene en ASAFINTECH se llama AML CONSULTING. Ofrece un servicio de la validación de listas negras. Ha creado una lista de personas en El Salvador, entonces ellos van acumulando la información a diario de todas las noticias, de los que caen presos, reportados por uno u otro motivo. | RegTech puede definirse como la tecnología que es utilizada para dar cumplimiento a las regulaciones. |
| 7 | ¿Los datos procesados por las RegTech son totalmente manejados en la nube? | Sí son manejados totalmente en la nube. En el caso de la RegTech que opera en el país, acumulan información pública que acumulan en la base de datos para que sean consultados por sus clientes. | Para poder funcionar, las RegTech utilizan la nube para almacenar la información que obtienen y de esta manera facilitar la disposición de la misma en el momento que se requiera. |
| 8 | ¿Existen empresas salvadoreñas que presten servicios de RegTech? | Si, por ejemplo, la empresa de RegTech que se tiene en ASAFINTECH es AML Consulting. Es una empresa que ofrece un servicio de validación de listas negras. Una de las partes de cumplimiento grande es el conoce a tu cliente (Know Your Costume) y conocer a tu cliente no solo es llenar un formulario, sino saber que es una persona de buena reputación, que no es un delincuente etc. El mecanismo que se utiliza a nivel mundial es que existen ciertas listas negras internacionales en las cuales si uno coloca el nombre de la persona o coloca la información que tiene de la persona, ahí uno puede ver si una persona está listada como alguien que lo busca alguna | En El Salvador, los servicios RegTech aún no se implementan a un nivel adecuado, se tiene solo una empresa que brinda el servicio de validación de listas negras, lo que es solo una de las funciones básicas que puede llegar a tener una RegTech bien desarrollada. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | autoridad o como alguien que ha tenido problema en el pasado, entonces cuando uno ve el tipo de problema o como está reportado uno decide si lo hace cliente o no. Esta RegTech lo que ha creado es una lista de personas en El Salvador, entonces ellos van acumulando la información a diario de todas las noticias de los que caen presos, de los que son reportados por uno u otro motivo, los ponen en esa lista y éstas pueden ser consultadas por los oficiales de cumplimiento para que tomen la decisión de hacerlo cliente o no. | |
| 9 | Si no existen empresas salvadoreñas que brinden servicios de RegTech, ¿cómo hacen las empresas internacionales para adaptar sus servicios de cumplimiento a la normativa nacional? | El problema de empresas internacionales es que no se adaptan. Por ejemplo, las listas negras internacionales, ellos sacan información de medios probablemente digitales, pero no tienen el dato local, entonces son muy generales y esa es la ventaja de una RegTech local, que puede tienen más detalle, pueden ir a comprar los diarios y ver las listas y hacen un chequeo mucho más preciso de los casos que van apareciendo o de las alarmas que van a ir apareciendo. Entonces una RegTech internacional tendría que tener oficinas en el país para poderse adaptar a los servicios locales, pero cuando son empresas muy globales les cuesta mucho. | Para que una empresa internacional que brinde servicios RegTech pueda funcionar en el país se hace necesario que se establezca una oficina local, pues se haría complicado para una empresa internacional adaptar en sus servicios las leyes aplicables en El Salvador. |
| 10 | ¿Cuáles son las RegTech que operan en El Salvador? | Hasta el momento solo existe AML Consulting. | Es la única empresa que brinda servicios RegTech identificada hasta el momento por ASAFINTECH. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 11 | ¿Cuáles son las áreas en las que se aplica RegTech dentro de las FinTech que operan en El Salvador? | El Know Your Costume o el conozca a su cliente es una de las etapas del cumplimiento regulatorio. | Según la respuesta de la pregunta anterior, solo se identifica una empresa que brinda servicios FinTech en El Salvador y sus servicios van enfocados a la validación en listas negras, que es una de las etapas del conozca a su cliente. |
| 12 | ¿Las RegTech utilizadas en nuestro país cuentan con la capacidad para adaptarse a nuevas regulaciones que pueden surgir en el futuro? | Todas las FinTech se pueden adaptar sin ningún problema. Los que tienen que evolucionar en realidad son los supervisores, las entidades gubernamentales que son las que se han quedado a un nivel tecnológico atrasado. Ellos tienen que tratar la manera de alcanzar la realidad de la tecnología y la realidad que estamos teniendo. Todas las empresas se pueden adaptar de nuestro entorno FinTech porque son empresas basadas en tecnología y en función que la tecnología avance pues invertir un poco más y adaptarse. | Una de las ventajas que hace a las FinTech más competitivas en el mercado financiero es la capacidad que tienen para adaptarse a las nuevas regulaciones que puedan imponer las entidades supervisoras, sin la necesidad de incurrir en costos desproporcionados. |
| 13 | ¿Cuáles son los riesgos asociados en el uso de RegTech? | Yo no le veo riesgos, al contrario, le veo beneficios de que está automatizando un proceso nuevo. Obviamente como toma presente tecnología y como toda tecnología, talvez los riesgos que pueda haber son los riesgos de ciberseguridad que todos conocemos, es decir que violen la seguridad para alcanzar las bases de datos, que violen la seguridad para utilizar esos servicios de una mala manera, pero en sí como servicio, creo que no ofrece un riesgo, lo que ofrece es una ventaja para automatizar un proceso. | El principal riesgo de las RegTech es la ciberseguridad, pues al ser aplicaciones que están basadas en tecnología y sus bases de datos permanecen en la nube, necesitan reforzar sus controles informáticos que permitan el resguardo de su información. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 14 | ¿De qué manera minimiza los ataques cibernéticos en las FinTech el uso de las RegTech? | Cada empresa debe establecer sus propios mecanismos y políticas de ciberseguridad. Hoy día, durante la pandemia y después de la pandemia los ataques de hackers a las instituciones que manejan gran cantidad de datos de clientes son más frecuentes, existe mucho ramsonware que cuando le roban el acceso a las empresas, les piden un rescate para devolverles el acceso, pero cada uno de los que maneja este tipo de plataforma tiene que establecer su propio plan de mitigación de riesgos, establecer un plan donde se pueda anticipar a un caso como este y poder establecer los mecanismos tecnológicos de seguridad de la información para evitar que sucedan. Ninguna plataforma es cien por ciento segura. | El establecimiento de un plan de mitigación de riesgos se vuelve esencial para prevenir que se den intrusiones, sin embargo, ningún control es infalible. |
| 15 | ¿Qué es SupTech y cómo funcionan? | Herramientas que utilizan los entes supervisores | Estas tecnologías brindan servicios de supervisión sobre la efectividad de los controles implementados por las RegTech. Estas tecnologías son utilizadas por las entidades supervisoras que son las encargadas de velar por el cumplimiento de las normas y regulaciones establecidas para la operatividad de las entidades financieras. |
| 16 | ¿La Superintendencia del Sistema Financiero utiliza la herramienta SupTech? | Lo desconozco. Mi percepción es que no porque la Superintendencia del Sistema Financiero no es tan avanzada en temas de tecnología. | La Superintendencia del Sistema Financiero se apoya de programas tecnológicos para realizar la labor de entes supervisores, sin embargo, estos programas no son tan avanzados como las tecnologías SupTech, pues sus procesos carecen de automatización. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 17 | Mencione las ventajas y desventajas de cada una de las Tecnologías: FinTech, RegTech y SupTech. | Desventajas no le encuentro. Las ventajas son que conocen mejor a los clientes y adaptan los servicios de una manera más eficiente, más específica para sus clientes que los bancos, que en realidad el sistema bancario podemos decir que se está quedando obsoleto. Hoy en día con lo que está pasando en El Salvador, con el lanzamiento de la Chivo Wallet que también es una FinTech patrocinada por el Gobierno y ha dejado demostrado que en muy corto tiempo puede llegar a tener millones de usuarios y tener una adopción masiva y puede tener un buen desempeño y abarca una inclusión de clientes que probablemente no ocupan el sistema financiero y van a empezar a usar un nuevo sistema financiero alternativo de una empresa como Chivo que ofrece este tipo de tecnología más cercana más comprensible, con más ventajas que la banca. | La principal ventaja que se identifica de estas tecnologías es la de alcanzar a un mayor número de usuarios en un menor tiempo, reforzando la inclusión financiera. |
| 18 | ¿Cuáles son los riesgos asociados en el uso de SupTech? | No puedo responder porque no se el detalle de este tipo de servicios. | |
| 19 | ¿La inclusión del Bitcoin a la economía salvadoreña supone la necesidad de acrecentar las regulaciones y supervisiones existentes? | Las FinTech cuando inician deben adaptarse a las regulaciones que existen. ¿Que tengan que tener regulaciones nuevas? Probablemente, puede haber regulaciones nuevas que se puedan implementar para cumplir ciertos aspectos. Posiblemente en el camino se pueden identificar ciertos espacios no cubiertos en la regulación que se tienen que complementar ya sea con normativas nuevas o con otras leyes y cubrir estos espacios. | Existe en El Salvador regulaciones ya establecidas que las empresas que operen con Bitcoin deben cumplir, por lo que dependerá de evaluaciones posteriores determinar si se necesitan reforzar o introducir nuevas regulaciones. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 20 | ¿Cómo pueden los supervisores fomentar la innovación y al mismo tiempo asegurar la existencia de una regulación apropiada? | Debería ser la responsabilidad que debe tener un ente supervisor, fomentar la innovación y al mismo tiempo controlar que no haya nuevos actores con malas intenciones y que puedan restringir y controlar que la industria FinTech o que cualquier sector financiero crezca sanamente. La Superintendencia muchas veces actúa más como un policía controlando y supervisando de una manera agresiva pero no permite o no incentiva la innovación. Estamos ante un escenario donde la superintendencia debe aprender más, modernizarse, inclinarse por la innovación manteniendo el equilibrio con la regulación. | Se vuelve fundamental que los entes supervisores establezcan medidas que mantengan el equilibrio entre la innovación y la regulación, pues si solo se establecen nuevas medidas reguladoras, se llega a limitar la capacidad para innovar los servicios financieros. |

*Nota:* Elaborado con base en las respuestas obtenidas por parte del representante de ASAFINTECH.

**Tabla 4**

*Resultados de la entrevista al profesional con experiencia en encargos de aseguramiento*

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| 1 | ¿Qué son las RegTech y las SupTech? | Son términos nuevos que están aplicados en el marco del surgimiento de lo que son las FinTech, que es la tecnología financiera aplicada a los servicios financieros. Así como son las FinTech requieren de un marco de actuación, un conjunto de normas y reglas que sean legales o técnicas y esas prácticamente están manifestadas en ese término que se llama RegTech que son las tecnologías aplicadas a las regulaciones o funcionamientos de las FinTech; es la regulación aplicando tecnología. Pero aparte de eso, como todos los sistemas requieren, primero diseño de regulaciones tanto legales como técnicas, también requieren que existan funciones adicionales para supervisar que esas normas, esas regulaciones estén incorporadas en los servicios FinTech, eso es lo que conocemos como SupTech, que no es más que la supervisión de la FinTech a través de medio tecnológico. | Las RegTech y SupTech son tecnologías que se complementan entre sí. Las RegTech se encargan de dar cumplimientos a las regulaciones que son aplicables a las empresas FinTech y las SupTech se encargan de validar que las RegTech den un cumplimiento efectivo de esas regulaciones. |
| 2 | ¿Cree usted que las herramientas RegTech y SupTech pueden ser utilizadas para desarrollar trabajos de auditoría forense? Si_____ No____ Explique: | Habría que ver que el tema de FinTech por el momento está aplicado solamente a entidades financieras, pero en el momento que muchas de las empresas de cualquier área de servicios, de producción o de canales de distribución, ya en si empiezan a generar sus propias aplicaciones para mejorar el servicio, desde ahí estamos incursionando en servicios FinTech, siempre y cuando se puedan | Dado que las regulaciones que deben cumplir las FinTech son manejadas por servicios o tecnologías RegTech, puede suponerse que la necesidad de una auditoría forense con enfoque detectivo se ve reducido, pues si los controles de las RegTech son efectivos, la posibilidad de que se dé un esquema de fraude es mínimo, sumado al doble control que se |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | monetizar todos estos servicios. Pensando en estas posibilidades de ejercer auditoría forense, primero para que se requiera auditoría forense es porque existe indicio de algún esquema de fraude o que ya se dio algún tipo de fraude, por lo tanto, estaríamos hablando que estaría fallando en el caso de las FinTech, ya sea el marco de regulación tecnológica que sería la RegTech. La SupTech en realidad utilizarlas para un marco de auditoría forense ya sería solamente para consultar procesos en relación a qué es lo que falló con las RegTech porque al final la regulación tecnológica es la que tiene que establecer el marco de actuación de las FinTech. Digamos que, si se puede utilizar, pero dado que el marco tecnológico de actuación ya estaría enfocado a otro tipo de auditoría forense que sería la auditoría forense informática, no la auditoría forense financiera. Entonces hay que irnos delimitando ya de que si se puede utilizar en el sentido de que la información que se pueda proveer es en línea. Aplicaría aquí un concepto adicional que hay que agregarle a la auditoría forense y sería un concepto nuevo que ha aparecido que sería continua y la auditoría continua prácticamente utiliza siempre recursos tecnológicos pero se va revisando o se va supervisando transacción por transacción, entonces desde ese punto de vista el enfoque seria preventivo, no detectivo porque se supone de que el marco de operación de las FinTech que serían el objeto de trabajo de un auditoría forense estaría dando ya fallas | implementa gracias a las SupTech, que son las que se encargan de recopilar y analizar la información que obtienen de las RegTech, ejecutando procedimientos de supervisión que permiten detectar desviaciones en los controles y advertir sobre la existencia de un posible fraude. Por lo tanto, la auditoría forense debe aplicarse con un enfoque preventivo, con el propósito de opinar sobre la razonabilidad y/o sugerir controles complementarios que contribuyan a la prevención de fraudes. Por lo expresado anteriormente, se asume que el auditor forense que se contrate para la realización de este tipo de encargo, necesita poseer conocimientos sobre la realización de una auditoría de sistemas, o valerse de un experto en el tema, pues se tendrán que aplicar procedimientos que permitan validar la efectividad de las RegTech y las SupTech. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | que serían identificables a través de las SupTech, entonces si es posible trabajar en un marco pero no es que la auditoría forense vaya a crear un nuevo marco o enfoque de auditoría porque todo esto estaría designado una especialidad de auditoría forense que es la auditoría forense informática. | |
| 3 | ¿Cuáles son las ventajas de utilizar las RegTech y las SupTech en una auditoría forense? | En realidad, estaríamos ante herramientas que al final quizás la auditoría forense no debería de ocurrir. Cuando estamos hablando sobre RegTech y de SupTech significa que las regulaciones están, las supervisiones serian casi inmediatas, por lo tanto, la posibilidad de una forense casi seria nula, porque tanto en la regulación tecnológica como la supervisión en línea deberían determinar cualquier fallo o desviación en relación las reglas establecidas en las FinTech. Llegar a un tema de auditoría forense por un hecho consumado sería bastante difícil, a menos que se trate de trabajar sobre una auditoría forense sobre una violación plena de los controles o de las RegTech que se hayan aplicado a una FinTech. Estaríamos hablando en esos casos, pero estaríamos quizás no en un caso de fallas de las FinTech, sino, un tema de ciberseguridad, donde le bajamos a ese entorno donde opera la FinTech y además de eso si todas las RegTech están definidas para las FinTech en cuestión no deberíamos llegar a un tema de auditoría forense, si talvez aplicar en un tema preventivo, pero no al termino de llegar a estar analizando hechos consumados. Le vería el tema de las ventajas en el | La ventaja principal del uso de estas tecnologías en una auditoría forense con enfoque preventivo aplicada a una FinTech recae en el hecho de que los procedimientos deben ir encaminados a validar o asegurarse que estas tecnologías posean una arquitectura adecuada, que sean capaz de efectuar controles automatizados y efectivos de tal manera que se dé cumplimiento a todas las regulaciones establecidas por las autoridades competentes para la prevención de fraudes dentro del ecosistema FinTech. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | sentido de que se puede preveer llegar a una auditoría forense como tal. Pero si tal vez trabajar en un tema de evaluación sobre efectividad de controles desde el punto de vista forense. Las ventajas más estarían en el tema de analizar la profundidad de alcance que tienen las regulaciones y el cumplimiento de la misma ya en la programación de la misma. | |
| 4 | ¿Conoce usted alguna firma o empresa que implemente el uso de las RegTech y SupTech? | Por el momento está ampliamente aplicado en el sistema financiero. Quienes están aplicando todo este tema de las SupTech y las RegTech prácticamente son los bancos y que tienen aplicaciones tecnológicas para desplegar el servicio financiero. SupTech más es de una aplicación y trabajo que realiza la Superintendencia del Sistema Financiero. De hecho, ellos hacen una supervisión antes de lanzar una aplicación al mercado. Se evalúa desde el punto de vista de la funcionalidad, desde el punto de vista de la ciberseguridad y también desde el punto de vista de la vulnerabilidad y la seguridad que brindan estos servicios a través de tecnologías financieras. Pero cuando estamos hablando de este tipo de empresas serían más las relacionadas a la parte del sector financiero; todavía otros sectores no entran en esto y otras empresas proveedoras de servicios financieros a través de tecnología que no necesariamente son bancos, acá tenemos por ejemplo empresas como pagadito que es la que utiliza el Centro Nacional de Registro y otros sistemas de pago para poder dar esos servicios financieros. Tenemos otra empresa que | Existen en El Salvador empresas que utilizan los servicios RegTech en su operatividad para el cumplimiento de las leyes y normativa aplicable. Sin embargo, los servicios que ofrecen estas RegTech en la actualidad son básicos, lo que no permite comprender la importancia de su implementación ni aprovechar las ventajas que éstas ofrecen.<br>El panorama que se tiene de las SupTech es el mismo de las RegTech. Hace falta invertir más en tecnología que permita simplificar procesos de supervisión por parte la Superintendencia del Sistema Financiero. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | moviliza dinero que es Tigo Money que es una FinTech que también al inicio no estaba con las regulaciones técnicas ni tampoco estaba bajo el esquema de supervisión de SupTech, sin embargo, ya eso se ha superado y entonces ahora son empresas que ya están bajo la consideración de las aplicaciones de estos conceptos de RegTech y SupTech. Por lo menos en el nivel del diseño que tiene a nivel de la Superintendencia del Sistema Financiero. Ya a nivel interno de estas empresas han desarrollado sus canales de supervisión y su marco de actuación tecnológica que es el que realmente utilizan para funcionar pero que deben estar permanentemente monitoreadas. | |
| 5 | ¿Cómo puede el auditor utilizar RegTech y SupTech como herramientas en la auditoría forense con enfoque preventivo? | Antes de poder presentar un enfoque de auditoría forense, cualquier auditor tendrá que empaparse (auditor con experticia en el área de tecnología) de cuales son todas esas regulaciones sobre una FinTech a la cual se le va a aplicar un enfoque preventivo. Independientemente de la FinTech que sea algunas tendrán buenas regulaciones, otras malas regulaciones. Para una auditoría forense preventivo que no es más que una consultoría, poder explicar y agregarle una serie de recomendaciones sobre los asuntos que la administración de las FinTech deben aplicar. | Debido a que este tipo de tecnologías centra sus servicios en el cumplimiento de las regulaciones, el auditor forense deberá verificar que dentro de sus parametrizaciones estén siendo incorporadas todas las regulaciones que le sean aplicable a la FinTech y de ser necesario, proponer recomendaciones para reforzar dichos controles. |
| 6 | ¿Cuál es la normativa técnica y legal aplicable a las | La normativa técnica y legal esta específicamente delimitada mas todo lo que tiene que ver en el marco del sistema financiero. Por la parte legal | Existe una serie de regulaciones que son aplicables a estas tecnologías y que son impuestas para todo el sistema financiero. |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | empresas que brindan servicios de RegTech y SupTech? | definitivamente tiene que haber una ley y la última que quieren entrar con servicios tecnológicos inclusivos es la ley bitcoin, aunque realmente no se refiere tanto a una aplicación y a un tema de tecnología financiera sino prácticamente abrir los canales para una inclusión financiera. En la parte técnica, como es una especialidad tecnológica se deben aplicar todas las normas de auditoría forense que corresponden a esa especialidad. Tendríamos una serie de marco de aplicación como COBIT, ITIL y otros marcos relacionados a esas áreas de desarrollo tecnológico. Se tendrían dos cuerpos, uno que es legal que sería diferente en cada país y otro que es el marco internacional que está basado en todas esas aplicaciones de auditoría para sistemas, más otros temas que tienen que ver con ciberseguridad que serían las normas técnicas aplicables que el auditor forense para FinTech considerando el RegTech y SupTech debería de conocer perfectamente. | Dependerá de los servicios que brinden cada FinTech la aplicación de una o varias de estas regulaciones. Por la parte normativa, al ser aplicaciones tecnológicas, les son aplicables marcos como los establecidos por COBIT e ITIL, que van encaminadas al desarrollo tecnológico. |
| 7 | ¿Considera necesario que las empresas FinTech apliquen herramientas como la RegTech y SupTech? Si_____ o No____ ¿Por qué? | De hecho, son el fundamento de trabajo. Si es necesario para hacer auditoría forense o tomarlas como herramientas es como lo básico. ¿por dónde vamos a empezar? Todo el marco RegTech y las consideraciones SupTech y a partir de ahí comenzar con un trabajo de consultoría forense. | Es la implementación de estas tecnologías lo que hace más competitivas a las Fintech, pues le permiten cumplir con las leyes sin tener que incurrir en gastos desproporcionados. |
| 8 | ¿Conoce usted si la Superintendencia de | Podríamos decir que esta afirmación podría tener una afirmación formal y otra afirmación real. Una | La Superintendencia hasta el momento no cuenta con un sistema de supervisión basado |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | Sistema Financiero utiliza las SupTech como herramienta de supervisión? | afirmación formal debería de ser que, la superintendencia de hecho es el ente supervisor y ellos deberían estar preparados para esto. Pero en la definición real la superintendencia todavía no ha desarrollado el marco de SupTech, tienen nociones, pero recordemos que esto requiere inversiones importantes en el área de tecnología, requiere capacitación de parte de las personas que van a estar trabajando en esto. Por ejemplo, cada día están saliendo nuevas aplicaciones financieras; va a sobrepasar la capacitad de la superintendencia en términos de regulación. Por ejemplo, en el país el mismo Banco Central de Reserva ha emitido unas recomendaciones en relación a las wallet que no sean supervisadas o que no sean descentralizadas o que sean custodiadas, pero sobre todo eso, la Superintendencia no tiene un marco de supervisión. Pero para todo eso la superintendencia no tiene un marco de supervisión. De hecho, ya con el tema de bitcoin ya encima de El Salvador, mucha gente está operando con los famosos trading y haciendo dinero con otras wallet que realmente no van a poder ser supervisadas por la Superintendencia. Tienen el marco formal pero ya en lo real hay cosas que difícilmente se pueden llegar a controlar porque todavía hace falta desarrollar eso. | en tecnología que pueda considerarse una SupTech, solamente hace uso de programas para ejecutar procedimientos mecanizados que aunque simplifiquen procedimientos, no son lo suficientemente sofisticados. |
| 9 | ¿Según su experiencia cual área consideraría de | El área de mayor riesgo sería el tema de ciberseguridad. Como son temas tecnológicos, la ciberseguridad incluye accesos físicos y lógicos, el | Debido a que las tecnologías SupTech y RegTech manejan sus bases de datos en la nube, la ciberseguridad se vuelve un factor de |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | mayor riesgo en una empresa FinTech? ¿Por qué? | tema de guardar secretos en relación la arquitectura de las tecnologías. Consideraría que el área de mayor riesgo es el área de la ciberseguridad tecnológica porque es ahí donde se presenta la mayor parte de vulnerabilidad en este tema, porque el tema de definir en qué va a consistir el servicio, saber dónde va registrado o no, todo eso es un tema de parametrización en esos sistemas. El área de la contaduría va a disminuir en el sentido que todas esas aplicaciones ya están parametrizadas. Pero esa ya es la operación normal, ósea decir hacer contabilidad detrás de una FinTech o tener un esquema de regulación sobre esa esa operación, en realidad todo eso escapa al control humano, pero todo lo que tiene que ver con la ciberseguridad, esa es la parte más vulnerable de todo este tema. Debemos comprender que el tema RegTech no es infalible, toda esta regulación técnica legal pues sabemos que ya está toda esa parte definida, pero es posible que ya una revisión en función de todas estas circunstancias que han acaecido lleve a revalorar el tema RegTech para esas aplicaciones que previamente hayan estado bajo riesgo. | riesgo muy significativo, pues en la actualidad ninguna plataforma puede ser considerada invulnerable a ataques cibernéticos, mucho menos las que son utilizadas en el sector financiero, pues son estas las que más atraen la atención de los hackers. |
| 10 | ¿Considera que los riesgos inherentes en una auditoría forense con enfoque preventivo se ven reducidos si la | Digamos que riesgos inherentes siempre van a existir, porque riesgos inherentes es el riesgo natural. El riesgo inherente en el caso de las FinTech no es el mismo riesgo que vemos cuando hacemos procesos manuales o semimecanizados, que son procesos que requieren la intervención humana. siempre van a | Los riesgos inherentes asociados a las FinTech no se eliminan con la utilización de las SuptTech y RegTech, solamente se trasladan a otras áreas, pues al ser servicios basados en tecnología, los riesgos se relacionan más con errores de parametrización, arquitectura del |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | FinTech hace uso de las herramientas RegTech y SupTech? | existir riesgos inherentes en el sentido de que el ámbito en el cual se desarrollan tiene riesgos naturales. Por ejemplo, el hecho que no haya un suministro energético a los supervisores que van a alojar toda la operación de las FinTech es un riesgo inherente bien grande en el país. Entonces a pesar de que estemos hablando de controles físicos o de suministros físicos de energía, si eso no está considerado a través de un RegTech entonces ahí tenemos un problema serio, entonces si se ven reducidos en el sentido que tanto el RegTech como el SupTech tengan una definición amplia en relación a las FinTech que estén tratando. Pero si toda la definición RegTech y SupTech para esas FinTech tienen un enfoque demasiado reducido, los riesgos inherentes van a ser bien grandes, porque no han considerado todos los riesgos posibles que se tengan. En la medida que se haga grande o pequeño y que el alcance sea suficiente así se van a disminuir los riesgos inherentes, pero no se van a reducir del todo porque siempre riesgos inherentes van a existir. | sistema, alimentación de la fuente, etc.; que son riesgos más identificados con el área informática. |
| 11 | ¿Qué tipo de procedimientos nos facilita la utilización de las herramientas RegTech y SupTech? | Casi la mayor parte de procedimientos que podrían aplicarse en esta área están definidos por softwares. No son los habituales procedimientos de auditorías que conocemos de prepare una cedula o verifique esa información, ese tipo de definiciones de procedimientos ya no son los que se aplican aquí. Por ejemplo aquí se va a utilizar software especializados | Con la utilización de estas tecnologías, los procedimientos de auditoría forense que se deben utilizar están orientados a los utilizados en una auditoría de sistema y por el tipo de información que se pone a disposición, deben aplicarse procedimientos encaminados a la validación de big data, para lo cual pueden ser |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | | en donde talvez el procedimiento ya esté definido y diga analice la integridad de la base de datos, que son conceptos ya de informática y que van a requerir procedimientos especializados en el área de IT, cuando ya se habla de integridad se está hablando de si todos los datos realmente están incluidos en la base de datos, si ha habido falla de traslados de tablas de un hacia otras, si las tablas están anidadas y facilitan un proceso de registro, si todo el tema de la RegTech aplicado ya en temas de validación de datos no tiene fallas; pero todo eso se hace a nivel informático, entonces ese tipo de procedimientos si facilitan en sentido que van al esquema RegTech y SupTech y toman todo lo que sea se haya definido, pero todas esas reglas se van a cargar en un software y no va a requerir tantos auditores, bastará uno con una especialización que llegue con su equipo especializado de alto rendimiento que le permita hacer una evaluación en relación a todo el tamaño de la FinTech. Los procedimientos si se facilitarían en la medida que todo el RegTech y el SupTech estén bien definidos y que todas esas reglas se puedan incorporar en el software de evaluación de la auditoría. | utilizados como herramientas de apoyo softwares especializados. |
| 12 | ¿Cuáles son los conocimientos específicos que debe poseer el profesional de auditoría para realizar un encargo | El primer conocimiento tiene que ser proficiente en el área de IT. Y en el área de IT tenemos especializaciones, por ejemplo, el área de diseño de software y otras especialidades que son en arquitectura de IT. Habrá otras especialidades que son más en el área de hardware, no tanto en tema de | Se vuelve necesario que el profesional que realice un encargo de auditoría forense con enfoque preventivo aplicado a una FinTech valiéndose del apoyo de la información obtenida de las SupTech y RegTech tenga conocimientos en el área de TI y posea |

| No. | Pregunta | Respuesta | Análisis |
|---|---|---|---|
| | de auditoría forense con enfoque preventivo aplicado a una FinTech? | programación que implica cableado, que implica un tema de conocer cuáles son las seguridades para los datacenter, seguridad lógica y física a niveles de acceso. A parte de conocer realmente el motivo principal por el cual funciona una FinTech, si va ser para servicios financieros o si va a ser para cualquier otro tipo de servicios. También deberá conocer exactamente con profundidad cual es el motivo principal de la existencia de esa FinTech. Podemos mencionar por ejemplo las FinTech que se utilizan para trasladar dinero de un país a otro, como el caso de Moneygram que todavía no se ha masificado porque todavía utiliza de intermediario los bancos, pero solamente examinar ahí implica conocer cuál es el lenguaje de programación, por lo tanto, ahí tenemos un mar de cosas que hay que aprender. Temas de controles informáticos, de rutina, de programación, etc. | experticia en la ejecución de auditorías de sistemas. |

*Nota:* Elaborado con base en las respuestas obtenidas por parte del profesional con experiencia en encargos de aseguramiento.

## 2.8 Diagnóstico de la investigación

Con los resultados obtenidos de las entrevistas realizadas, se procedió a elaborar un diagnóstico, para analizar si la utilización de las herramientas SupTech y RegTech facilitan la realización de auditorías forenses con enfoque preventivo aplicadas a empresas FinTech que operan en el área metropolitana de San Salvador.

Debe considerarse que el ecosistema FinTech en El Salvador está en pleno desarrollo, pues las empresas que brindan este tipo de servicios, en la actualidad se enfocan más en las verticales de pago, que son un servicio base para que una empresa sea considerada FinTech, pero el potencial de éstas se debe a otros servicios más innovadores como por ejemplo el Crowfunding, compra y venta de criptomonedas, entre otros.

Un factor importante a resaltar de las respuestas obtenidas por los profesionales, es que no se considera fundamental la creación de una ley FinTech, pues existen regulaciones que son aplicables a éstas según la vertical en la que se clasifiquen.

Por lo expresado anteriormente, se debe interpretar que, en lo que respecta a las soluciones que brinden las RegTech y SupTech deberán adaptarse a las regulaciones aplicables a cada FinTech, por ejemplo, los establecidos en las Normas de Debida Diligencia del GAFI.

Aunque en la actualidad no se utilicen los servicios SupTech y solo se tenga una RegTech que brinda servicios de validación de listas negras, por sus definiciones y características se pueden identificar las ventajas que éstas brindan en la realización

de una auditoría forense, pues constituyen los medios de consulta o de validación para verificar la efectividad de controles implementados por las FinTech para la prevención de fraudes.

Sin embargo, debido a que las SupTech y las RegTech son herramientas que funcionan a base de tecnología, se vuelve necesario que el auditor forense que se auxilie de estas herramientas posea experticia en la realización de autorías de sistemas. Además, debe considerar que los riesgos de ciberseguridad se vuelven mucho más significativos, por lo que debe implementar procedimientos que le permitan no solo validar que se esté dando cumplimiento con la normativa legal aplicable, sino que se poseen los mecanismos para evitar que se violen los controles de seguridad para evitar infiltraciones a las bases de datos.

Actualmente, existen pocos profesionales que conocen sobre el funcionamiento de las herramientas RegTech y SupTech que son aplicadas por las FinTech para el cumplimiento normativo y legal, sumado al hecho que no se tienen antecedentes de auditorías forenses sobre casos de fraudes dentro de este ecosistema en el que se hayan auxiliado de los reportes que brindan estas herramientas.

Por tal motivo, la realización de este trabajo investigativo es fundamental para que los lectores puedan conocer y/o ampliar sus conocimientos en cuanto al funcionamiento de estas tecnologías y cómo pueden facilitar las labores de obtención de datos que serán sujetos a análisis por parte del auditor forense.

## 2.9 Marco Teórico y Conceptual de las SupTech y RegTech.

Se incluye este apartado como complemento para un mejor entendimiento del funcionamiento de las herramientas SupTech y RegTech, además se presentan algunos lineamientos que deben ser considerados al plantear los programas de auditoría.

### 2.9.1 Descripción de las RegTech y sus diferentes enfoques

Las soluciones que pueden dar son diversas, cada una busca dar soluciones a un área en específico, por lo que éstas pueden clasificarse según su enfoque de aplicación de la siguiente manera:

- **Enfocada al cumplimiento de la normativa KYC:**

  En atención a los requerimientos que tienen las instituciones financieras de cumplir con procedimientos y controles para valorar, identificar y verificar la identidad de sus clientes y beneficiarios finales, así como el monitoreo de sus operaciones con el fin de gestionar el riesgo de lavado de dinero y financiamiento al terrorismo.

  La NRP-08 emitida por el BCR proporciona la guía de medidas que el auditor forense debe tener presente al evaluar la eficiencia del cumplimiento normativo de este tipo de RegTech y que según el artículo 18 de esta normativa las medidas son las siguientes:

  a) Identificar al cliente de forma fehaciente mediante sus documentos de identidad y otra información básica que las entidades solicitan al momento de la contratación, cerciorándose que el documento sea original. En el caso de las

personas jurídicas, aparte de identificarlas, deberán también conocer y documentar su naturaleza jurídica, razón social, actividad económica a la que se dedica, acreditación e identificación del representante legal, accionistas y socios con una participación patrimonial arriba del 10% y miembros de la Junta Directiva, entre otros. Debiendo conocer adecuadamente la actividad económica que desarrollan sus clientes, su magnitud, frecuencia, características básicas de las transacciones en que se involucran corrientemente, establecer que el volumen, valor y movimiento de fondos de sus clientes guarden relación con la actividad económica de los mismos;

b) Verificar listados actualizados de personas naturales o jurídicas involucradas en delitos relacionados con el lavado de dinero o financiamiento al terrorismo, provenientes de publicaciones de países u organismos locales e internacionales.

c) Verificar listados relacionados con países considerados jurisdicciones de nula o baja imposición fiscal, personas naturales o jurídicas vinculadas con actos delictivos, incluido el terrorismo y que desempeñan o han desempeñado funciones públicas destacadas en el país o el país de origen, previo a establecer o iniciar cualquier negocio financiero con clientes potenciales.

d) Solicitar documentación de acuerdo con el nivel de riesgo LD/FT, sobre el origen de los fondos, activos o mercaderías depositados por el cliente.

e) Establecer perfiles transaccionales de los clientes sobre las operaciones y servicios que realizarán con la entidad, en base a su actividad económica;

f) las entidades deben identificar a los beneficiarios finales en todas las transacciones u operaciones realizadas por éstos;

g) Establecer procedimientos continuos para actualizar información general de los clientes existentes;

h) Mantener un registro detallado de los clientes de la entidad que han generado reportes de operaciones sospechosas;

i) Monitorear las transacciones realizadas por los clientes durante el curso de la relación comercial, con el fin de asegurar que las transacciones que están haciendo son consistentes con su perfil transaccional; y,

j) Monitorear permanentemente a clientes o usuarios que se encuentran en países o jurisdicciones designados como de alto riesgo o no cooperantes por el GAFI, o que tienen negocios con personas ubicados en estos territorios; asimismo, a clientes o usuarios que realizan negocios financieros en países considerados de baja o nula tributación fiscal.

- **Enfocada en el reporting regulatorio.**

Es normal que las instituciones financieras tengan la necesidad de estar compartiendo distintos tipos de reportes e informes a los entes supervisores cada cierto tiempo, por lo que este tipo se encarga de transmitir a los entes supervisores los distintos reportes que son requeridos según la legislación de cada país.

- **RegTech (AML)**

  Las instituciones financieras están obligadas a prevenir el lavado de dinero, por lo que se hace necesario que estas instituciones consideren como uno de sus principales controles la contratación de servicios RegTech. Una AML tiene la necesidad de ampliar su capacidad de cumplimiento normativo y regulatorio. Sus servicios incluyen procesos de conocimiento de clientes, verificación de documentación, monitoreo de procesos automatizados, incluyendo un cálculo de perfil de riesgo que se establece mediante el análisis de transacciones y chequeo continuo de listas internas y externas.

### 2.9.2 Criterios para seleccionar una RegTech por parte de una FinTech

Existen algunos criterios que deben ser considerados por las entidades en estudio al momento de seleccionar otra de regulación tecnológico y que son los mismos que deben considerar los bancos. Según COBIS (Solis, 2017)[1] estos puntos deben ser:

- Puedan manejar datos robustos y ofrecer una reportería útil para los tomadores de decisiones de sus instituciones.

- Entiendan el ecosistema regulatorio al que se rige un banco y que estén dispuestos a diseñar las soluciones necesarias para cumplirlo.

[1] **COBIS:** Es una empresa de desarrollo de soluciones financieras que cuenta con experiencia tato en el mundo regulatorio del sector bancario, como en el desarrollo de tecnologías flexibles que se adapten a los requerimientos de cada institución.

- Explorar soluciones de inteligencia artificial que ayuden a reducir el riesgo.
- Invertir en seguridades de almacenamiento de datos que disminuyan el riesgo de cumplimiento.
- Proveedores de soluciones RegTech que ofrezcan flexibilidad para adaptarse a las necesidades del banco y los cambios regulatorios rápidos en la industria.
- Evaluar el ecosistema digital de sus proveedores enfocándose en las FinTech que posean blogs de tecnología donde compartan las actualizaciones regulatorias emergentes en el sector.

### 2.9.3 Tecnologías implementadas por las RegTech y SupTech

Las de carácter regulatorio implementan diversos tipos de tecnologías que son las que permiten potenciar sus servicios mediante la automatización y agilización de sus procesos. Entre las principales tecnologías involucradas se identifican las siguientes:

- **IA (Inteligencia Artificial)**

  Aunque este tipo de tecnología aún no se encuentre desarrollada en su totalidad, los beneficios que actualmente brinda son muy provechosos para las empresas, pues mediante su implementación se logra resoluciones de problemas en menor tiempo y con una reducción de costos significativos. En el caso particular de las RegTech, dependiendo del área de aplicación utilizará un nivel de IA más avanzado que otras, es decir, su programación puede estar basada en

reglas o aplicar sistemas que piensan como humanos; tal es el caso de las redes neurales artificiales que son capaces de aprender modificándose automáticamente entre sí, lo que permite automatizar funciones para las cuales anteriormente era necesaria la intervención humana.

- **Big Data**

  Es una tecnología complementaria a las IA, pues permite la acumulación de una gran cantidad de datos que pueden ser gestionados y mediante el apoyo de otras herramientas éstos puedan ser analizados y visualizar resultados por medio de informes. Es gracias a la implementación de esta tecnología que las RegTech pueden almacenar la información recopilada y tenerla disponible para que sea analizada por los entes supervisores mediante las SupTech.

- **Ciberseguridad**

  Evitar los ataques cibernéticos, proteger la información, evitar fraudes y tener una jerarquización más efectiva resulta crucial para quienes manejan información sensible. Las entidades financieras requieren sistemas seguros de prevención y actuación contra hackers y cibercriminales. Firmas como Dokify, Enigmedia, Coocket, Blueliv, Simarks y Smartdefense actúan en este ramo. De acuerdo con lo anterior, uno de los principales objetivos de las SupTech es supervisar la digitalización de los procesos de información y regulación minimizando los riegos antes mencionados.

- **Compliance**

  Es la tecnología que permite la aparición de las tecnologías de regulación y supervisión, pues están encaminadas al cumplimiento legal a base del uso de tecnologías. La importancia del compliance durante los últimos años ha tomado mayor relevancia, por lo que cada una de estas soluciones se ha ido perfeccionando y agrupando en una sola herramienta tecnológica, conocida como RegTech. Complementario a ésta aparece SupTech que sirve de doble filtro para la validación del cumplimiento de las regulaciones.

- **Digital onboarding**

  Dado que las FinTech pueden recopilar información mediante la RegTech, como es el caso de las aplicadas con enfoque Know Your Customer y de forma complementaria la SupTech asegura mediante la supervisión que los usuarios accedan a todos los servicios y productos que una entidad pueda ofrecer, digital onboarding permite a través de su proceso central la incorporación de clientes y usuarios de una forma ágil, sencilla, segura. Esta parte fundamental de la relación usuario-organización se presenta como el momento clave para dos aspectos fundamentales: la seguridad de la empresa u organización de adquirir como cliente a un usuario legítimo con garantías y con los controles apropiados y la decisión final del cliente potencial de pasar o no a ser cliente (eID, 2021).

### 2.9.4 Ventajas de la utilización de SupTech y RegTech para el auditor forense

La utilización de estas herramientas permite al auditor sacar provecho de los datos que puede obtener de éstas. Entre las principales ventajas se pueden mencionar las siguientes:

- **Información oportuna.** En las auditorías tradicionales, la obtención de la información puede llegar a generar retrasos en la ejecución del trabajo, pues depende de las personas encargadas de la entidad auditada recopilar y/o actualizar la información requerida para la obtención de evidencia de auditoría que permita fundar una opinión. Con la implementación de las herramientas SupTech y RegTech por parte de las empresas FinTech, se evitan estos inconvenientes, pues los datos que recopilan estas herramientas son almacenados en la nube, lo que hace más sencilla su obtención y permite reducir tiempo en la ejecución del encargo.

- **Información adecuada.** Los informes que se obtienen de estas herramientas, siempre que haya evaluado previamente su fiabilidad, permite al auditor contar con información soporte adecuada sobre la cual puede fundar su opinión.

- **Análisis de la población.** Con la base de datos que es manejada en la nube, se facilita la aplicación de técnicas de auditoría aplicadas a una Big Data, lo que conlleva al análisis de toda la población, sin tener que recurrir a opinar sobre una muestra.

- **Verificación de operaciones en tiempo real.** Las RegTech incluyen dentro de sus funciones el monitoreo de transacciones en tiempo real, lo que facilita la aplicación de pruebas dirigidas que permitan validar la efectividad de los controles que son implementados para detectar y prevenir fraudes.

- **Informe de alertas.** Luego que el profesional ejerciente obtenga evidencia de que los informes sobre alertas que generan las RegTech son fiables, puede apoyarse de estos informes para evaluar el nivel de riesgo al que la FinTech se enfrenta y obtener una seguridad razonable de que los controles implementados por estas entidades con el apoyo de la herramienta de regulación tecnológica son adecuados para prevenir fraudes.

### 2.9.5 Validación y evaluación de los sistemas

Antes de que el auditor forense plantee sus procedimientos para verificar si los controles implementados por las FinTech son adecuados para la prevención de fraude, debe tener la seguridad de la integridad y veracidad de los reportes generados por las herramientas tecnológicas.

Es necesario que el auditor contratado para realizar una auditoría forense con enfoque preventivo aplicado a una FinTech conozca de la auditoría en sistemas o se auxilie de un profesional en la materia, pues tendrá que efectuar con antelación una serie de procedimientos que le permitan determinar la confiabilidad de la información que obtendrá de las bases de datos que le sean proporcionados.

Según la IFAC[2] para realizar una auditoría de sistemas, el profesional debe contar con los conocimientos que se detallan en la tabla 5.

[2] Federación Internacional de Contadores. Para contribuir al fortalecimiento de la profesión contable emite la Declaración de Prácticas de Educación Internacional 2 titulada: Tecnología de la Información para Contadores Profesionales, documento que puede ser consultado en el sitio web: http://www.ifac.org

**Tabla 5**

*Conocimientos generales de los temas TI*

| Competencias | Temas |
|---|---|
| **Estrategia de Tecnología de la Información** | |
| Los candidatos pueden explicar, describir o discutir la importancia de alinear la estrategia de TI con estrategia de negocio. | Estrategia empresarial y la visión.<br>Entorno de TI actual y futuro.<br>La planeación estratégica de Gobernabilidad en curso y los resultados de la vigilancia. |
| **Tecnología de la Información Arquitectura** | |
| Los candidatos pueden explicar, describir o discutir cómo la arquitectura de TI se refiere a la entidad de modelo de negocio. | Conceptos de los sistemas generales<br>Procesamiento de transacciones en los sistemas de negocio<br>Los componentes de hardware<br>Software<br>Protocolos, normas y tecnologías de apoyo<br>Métodos de organización de datos y de acceso<br>Profesionales de TI |
| **TI como un habilitador de procesos de negocio** | |
| Los candidatos pueden explicar, describir o discutir cómo los impactos de TI en el modelo de negocio y procesos de negocio y los riesgos asociados. | Las partes interesadas y sus necesidades<br>Modelos de negocio de la entidad<br>Los riesgos y oportunidades relacionados con IT<br>Impacto de las TIC en los modelos de negocio, procesos de la entidad y soluciones |
| **Sistemas de Adquisición / Proceso de Desarrollo** | |
| Los candidatos pueden explicar, describir o discutir las etapas de la | Sistemas de adquisición / desarrollo fases del ciclo de vida, las tareas |

| | |
|---|---|
| adquisición de sistemas y proceso de desarrollo y comprender el papel del contador dentro de ella. | Estudios de investigación y de viabilidad<br>El análisis de requerimientos y el diseño inicial<br>El diseño de sistemas, selección, adquisición / desarrollo<br>Implementación de Sistemas<br>Programa de mantenimiento y sistemas de cambios<br>La gestión de proyectos, planificación de proyectos, control de proyectos métodos y normas. |
| **Gestión de Tecnologías de la Información** | |
| Los candidatos pueden explicar, describir o discutir:<br>(A) cómo se gestiona dentro de una organización, con un enfoque en los sistemas de contabilidad,<br>(B) monitoreo del desempeño, y<br>(C) el cambio gestión y los procedimientos para la actualización hardware y software. | Organización de TI<br>Gestión de las operaciones de TI, la eficacia y la eficiencia<br>Gestión de activos de TI<br>Gestión de la seguridad de TI<br>La supervisión del rendimiento y el control financiero de TI recursos<br>Software para uso profesional |
| **Comunicación y TI** | |
| Los candidatos pueden explicar, describir o Los candidatos pueden explicar, describir o discutir de TI, y los beneficios y riesgos de TI, en relación con comunicación. | Conceptos generales de la comunicación de TI<br>Redes y datos electrónicos de transferencia<br>Los riesgos en la comunicación con el apoyo de TI |

*Nota:* Tomado del informe: Tecnología de la Información para Contadores Profesionales.

Los elementos que el auditor debe evaluar en materia informática son los siguientes:

- Mecanismos de seguridad para una adecuada arquitectura.
- Mecanismos de firewall establecidos en la red pública y privada de la organización
- Proceso de identificación de los usuarios.
- Utilización de firmas electrónicas.
- Infraestructura para manejar y controlar las claves públicas y sus certificados correspondientes.
- Logs de aplicación monitoreados por personal responsable.
- Métodos y procedimientos para reconocer las violaciones de seguridad.
- Medidas para asegurar la confiabilidad de los usuarios.

Para la evaluación de estos aspectos el auditor puede auxiliarse de las siguientes técnicas:

- Documentación: Deben analizarse los contratos de servicios RegTech para validar que se estén ejecutando los servicios acordados, evaluar que la FinTech esté cumpliendo con los términos y condiciones que son aceptados por los clientes y cualquier otro tipo de documentación de interés.
- Observación: Para lo que se requiere apoyarse de procedimientos de recopilación, análisis e interpretación de datos.
- Re-ejecución: Estas técnicas están basadas en pruebas de penetración para evaluar los mecanismos de seguridad.

### 2.9.6 Ciberseguridad y Big Data

La seguridad es uno de los aspectos más importantes en las entidades financieras y para el caso de las FinTech, la seguridad de sus datos presenta un mayor riesgo de ciberataques por estar totalmente manejados en la nube; por lo que el auditor deberá cerciorarse que este tipo de empresas contraten los servicios de resguardo de información por parte de empresas que posean protocolos de seguridad avanzados.

Deben ejecutarse procedimientos que permitan validar la efectividad de los controles de ciberseguridad, como por ejemplo pruebas de penetración; sin dejar de lado la aplicación de la ISO 27001, que da un panorama amplio sobre las medidas que deben tomar las organizaciones para la gestión de seguridad de la información, por lo que el auditor forense debe elaborar programas enfocados a la revisión del cumplimiento de estos controles y validar que sean adecuados.

En lo que respecta al Big Data, los procedimientos que se ejecuten deben considerar procesos para validar la calidad de los datos, el manejo y los reportes generados. Para esto puede utilizarse la matriz de controles que se detallan en la tabla 6 de este documento:

**Tabla 6**

*Matriz de controles para una auditoría de Big Data*

| Objetivo de Control | Descripción |
|---|---|
| El manejo de la seguridad de la información es parte de la estrategia de Big Data | 1. Un programa de ciberseguridad existe dentro de la organización a fin de combatir amenazas internas/ externas,<br>2. Aquellas aplicaciones capaces de eludir el sistema operativo, la red y los controles de aplicación se encuentran prohibidos y/o controlados apropiadamente,<br>3. El uso de aplicaciones de auditoría se encuentra acotado/segmentado a fin de evitar el mal uso y/o destrucción de los datos. Los Log de datos son revisados de forma periódica a fin de detectar actividades sospechosas,<br>4. Todos los servicios que están basados en la nube dentro de la organización se encuentran aprobados para el uso y almacenamientos de los datos de la organización,<br>5. El área de IT evalúa la seguridad de los proveedores de servicios relevantes,<br>6. Existe un proceso formalizado para el proceso de administración de "parches" de los sistemas asegurando que son actualizados con las últimas versiones, las cuales fueron aprobadas de forma oportuna |
| El manejo de la seguridad de los datos es parte de la estrategia de Big Data | 1. Sólo los usuarios del negocio autorizados tienen acceso a los datos y los reportes de los grandes sistemas de datos (Big Data),<br>2. Solo un acotado número de usuarios técnicos tiene acceso privilegiado a los grandes sistemas de datos, incluido los sistemas operativos, redes, bases de datos y aplicaciones,<br>3. Los accesos a los grandes sistemas de datos son revisados de forma periódica para asegurar que sean los apropiados, |
| El acceso de terceras partes debe ser manejado de forma apropiada | 1. Los requisitos contractuales y regulatorios del proveedor son analizados y tratados antes de conceder el acceso a los datos y sistemas de información, |
| La privacidad de los datos debe ser parte de la estrategia de Big data | 1. Los datos son inventariados y clasificados para asegurar que los datos críticos de la organización, incluida la información personal, estén debidamente protegidos, |

| Objetivo de Control | Descripción |
|---|---|
| | 2. Existe documentado, aprobado e implementado un proceso de respuesta a incidentes para asegurar que la brecha de datos es manejada apropiadamente. |

*Nota:* Auditando Big Data, por Javier Fernando Klus https://www.auditool.org/blog/auditoría-de-ti/5559-auditando-big-data

### 2.9.7 Lineamientos para la verificación de fraudes.

Tal como lo establece el instructivo de la Unidad de Investigación Financiera para la prevención del Lavado de Dinero y activos, el Financiamiento al Terrorismo y Proliferación de Armas de Destrucción Masiva, en adelante Instructivo-UIF-Prevención-LDA/FT/FPADM son las instituciones obligadas las que deben establecer sus políticas que permita prevenir, controlar y detectar las operaciones inusuales con respecto a sus clientes y usuarios, para lo cual necesitan realizar la debida diligencia de éstos, controlar sus operaciones y gestionar los riesgos asociados a los delitos de LDA/FT/FPADM.

Como se mencionó en párrafos anteriores, existen RegTech que se encargan de apoyar en el cumplimiento de las medidas establecidas para la realización de la debida diligencia del cliente. Pero estos procedimientos no son suficientes para la prevención de fraudes. Es necesario que una vez aceptado un cliente se implementen medidas para detectar operaciones inusuales y según lo establece el art. 36 del Instructivo-UIF-Prevención-LDA/FT/FPADM estas medidas deben ser, entre otras, las siguientes:

a) Determinar patrones de comportamiento y transaccionalidad usual del cliente o contraparte;

b) Monitoreo y control de señales de alerta;

c) Conocimiento y control de las características del mercado en el que se desarrolla la actividad económica del cliente o contraparte;

d) Conocimientos de los métodos utilizados para el LDA/FT/FPADM;

e) Capacitación a los empleados sobre los instrumentos para la detección de operaciones inusuales.

Es de aclarar que este tipo de medidas están enfocadas en los servicios bancarios tradicionales, pero pueden ser adoptadas por las FinTech como normas de buenas prácticas.

En El Salvador, a partir del 7 de septiembre de 2021 entró en vigencia la Ley del Bitcoin, lo que conlleva a la necesidad de aplicar controles específicos para la detección de fraudes que se pueden generar con el uso de criptomonedas.

Para controlar estos riesgos, el GAFI ha emitido un informe en el que propone una serie de alertas que deben tenerse en cuenta al establecer los controles para la prevención del lavado de dinero y financiamiento al terrorismo. Estas alertas están clasificadas como se detallan en la tabla 7.

**Tabla 7**

*Señales de alertas de Activos Virtuales*

| Señales | Indicador | Metodologías |
|---|---|---|
| Señales de alerta relacionadas con las operaciones | Tamaño y frecuencia de las operaciones | Estructurar operaciones de activos virtuales (AV) en pequeñas cantidades, o en cantidades por debajo de los umbrales de mantenimiento de registros o informes. |
| | | Realizar múltiples operaciones de alto valor. |
| | | Transferencia inmediata de AV a múltiples proveedores de servicios de activos virtuales (VASP). |
| | | Depositar AV en una oficina de cambios y luego convertirlos en otros AV que diversifiquen su cartera sin una explicación lógica comercial. |
| | | Aceptar recursos sospechosos de ser robados o fraudulentos. |
| Señales de alerta relacionadas con los patrones de operación | Operaciones relativas a nuevos usuarios | Realizar un gran depósito inicial para abrir una nueva relación con un VASP, mientras que el monto financiado es inconsistente con el perfil del cliente. |
| | | Realizar un gran depósito inicial para abrir una nueva relación con un VASP y financiar el depósito completo el primer día que se abre. |
| | | Un nuevo usuario intenta negociar el saldo completo de los AV, o retira los AV e intenta enviarle saldo completo fuera de la plataforma. |
| | Operaciones relativas a todos los usuarios | Operaciones que involucran el uso de múltiples AV, o múltiples cuantas, sin una explicación comercial lógica. |
| | | Hacer transferencias frecuentes en un período de tiempo determinado. |
| | | Operaciones entrantes de muchas carteras no relacionadas en cantidades relativamente pequeñas con transferencias posterior a otra cartera o cambio completo por moneda fiduciaria. |

| Señales | Indicador | Metodologías |
|---|---|---|
| Señales de alerta relacionadas con los patrones de operación | Operaciones relativas a todos los usuarios | Realizar un cambio de moneda VA-fiduciaria con una pérdida potencial. |
| | | Convertir una gran cantidad de moneda fiduciaria en AV, o en una gran cantidad de un tipo de AV en otros tipos de AV, sin una explicación lógica. |
| | | Operaciones de un cliente que involucran más de un tipo de AV y especialmente aquellos AV que brindan mayor anonimato. |
| Señales de alerta relacionadas con el anonimato | | Mover un AV que opera en una cadena de bloques pública y transparente, a un intercambio centralizado y luego intercambiarlo inmediatamente por una criptomoneda de anonimato o moneda privada. |
| | | Clientes que operan como un VASP no registrado. |
| | | Actividad transaccional anormal de AV cobrados en intercambios de carteras asociadas a la plataforma P2P sin una explicación comercial lógica. |
| | | AV transferidos hacia o desde carteras que muestran patrones previos de actividad asociados con el uso de VAS que operan servicios de mezcla o caída o plataformas P2P. |
| | | Operaciones que hacen uso de servicios de mezcla y rotación. |
| | | Recursos depositados o retirados de una dirección o cartera de AV con enlaces de exposición directa e indirecta a fuentes sospechosas conocidas. |
| | | Uso de carteras de papel o hardware descentralizados / no alojados para transportar AV a través de las fronteras. |
| | | Usurarios que ingresan a la plataforma VASP habiendo registrado sus nombres de dominio de Internet a través de proxis o usando registradores de nombres de dominio que suprimen o censuran a los propietarios de los nombres de dominio. |

| Señales | Indicador | Metodologías |
|---|---|---|
| Señales de alerta relacionadas con el anonimato | | Una gran cantidad de carteras AV aparentemente no relacionadas, controladas desde la misma dirección IP. |
| | | Uso de AV cuyo diseño no está adecuadamente documentado y como los esquemas Ponzi. |
| | | Recibir o enviar a los recursos a los VASP cuyos procesos de DDC o conocimiento de su cliente son débiles o inexistentes. |
| | | Uso de cajeros automáticos/ quioscos AV que poseen tarifas de operación más elevadas o que estén en lugares de riesgo donde ocurren más actividades delictivas. |
| | | Crear cuentas separadas bajo nombres diferentes. |
| Señales de alerta sobre remitentes o beneficiarios | Irregularidades observadas durante la creación de la cuenta | Transacciones iniciadas desde direcciones IP que no son de confianza. |
| | | Intentar abrir una cuenta frecuentemente dentro del mismo VASP desde la misma dirección IP. |
| | | Sobre los usuarios corporativos/comerciales, sus registros de dominio de Internet se encuentran en una jurisdicción distinta que a su establecida. |
| | | Información KYC incompleta o insuficiente. |
| | Irregularidades observadas durante el proceso de DDC | Falta de conocimiento de remitente/beneficiario o proveer información imprecisa sobre la transacción. |
| | | Proporcionar documentos falsificados. |
| | | Identificación o credenciales de una cuenta compartidas con otra cuenta. |
| | Perfil | Discrepancias entre las direcciones IP asociadas con el perfil del cliente y las direcciones IP desde las cuales están siendo iniciadas las transacciones. |
| | | La dirección de AV de un cliente aparece en foros públicos asociada con actividades ilegales. |

| Señales | Indicador | Metodologías |
|---|---|---|
| Señales de alerta sobre remitentes o beneficiarios | Perfil | Un cliente es conocido a través de información pública disponible por fuerzas de orden público debido a una asociación criminal previa. |
| | | El remitente parece no estar familiarizado con la tecnología AV o soluciones en línea de custodia de cartera. |
| | Perfil de potenciales mulas de dinero o víctimas de estafa | Un cliente considerablemente mayor que la edad promedio de los usuarios de la plataforma abre una cuenta y participa en un gran número de transacciones. |
| | | Cliente que es una persona financieramente vulnerable. |
| | | Compra de grandes cantidades de AV no justificado por su patrimonio disponible. |
| | | Cambio frecuente de su información de identificación. |
| | Otros comportamientos inusuales | Intento de ingreso a uno o varios VASP desde diferentes IP de manera frecuente en el transcurso del día. |
| | | Uso de lenguaje en los campos de mensajes de AV. |
| | | Realización de transacciones repetidamente con un conjunto de personas con ganancias o pérdidas significativas. |
| | | Realizar transacciones con cuentas de AV o tarjetas bancarias que están conectadas con esquemas conocidas de fraudes. |
| Señales de alerta en la procedencia de recursos o patrimonio | | Transacciones de AV que se originaron o están destinadas a servicios de apuestas en línea. |
| | | Uso de una o varias tarjetas de crédito o débito que están vinculadas a una cartera de AV para retirar grandes cantidades de divisas fiduciarias. |
| | | Los depósitos a una cuenta o a una dirección de AV que es considerablemente mayor que lo común con una procedencia desconocida de recursos, seguido por una conversión a una divisa fiduciaria. |

| Señales | Indicador | Metodologías |
|---|---|---|
| Señales de alerta en la procedencia de recursos o patrimonio | | Falta de transparencia o información insuficiente sobre el origen y titulares de los recursos. |
| | | Recursos del cliente que provienen directamente de servicios de mezcla de terceros o de tumblers de cartera. |
| | | La mayor parte del origen del patrimonio de un cliente se deriva de inversiones en AV, Ofertas Iniciales de Monedas y Ofertas Iniciales de Monedas fraudulentas. |
| | | La fuente del patrimonio de un cliente se obtiene de manera desproporcionada de AV originados de otros VASP que carecen de controles. |
| | | Los recursos del cliente se originan o se envían a un cambiario que no está registrado en la jurisdicción donde está localizado el cambiario o el cliente. |
| Señales de alerta relacionadas con riesgos geográficos | | El cliente utiliza un cambiario de AV en una jurisdicción de alto riesgo. |
| | | El cliente envía recursos a VASP que operan en jurisdicciones que no tienen regulaciones para AV. |
| | | El cliente establece o reubica oficinas a jurisdicciones que no tienen regulaciones o que no han implementado regulaciones que gobiernen los AV. |

*Nota:* Informe del GAFI sobre Activos Virtuales Señales de alerta de LD/FT

En el Informe sobre casos y Tipologías Regionales del GAFILAT[3] se ilustran los flujogramas que describen el funcionamiento de los casos del lavado de dinero proveniente del tráfico ilícito de drogas por medio de monedas virtuales y los esquemas basados en pirámides financiera (esquema Ponzi) por medio de monedas virtuales.

[3] **GAFILAT:** Grupo de Acción Financiera para América Latina.

Las RegTech implementan procedimientos de alertas, por lo que al ejecutar la auditoría forense de una FinTech que presta servicios basado en criptomonedas, es necesario que el profesional evalué que los procedimientos realizados sean adecuados y atiendan las directrices de alertas establecidas por el GAFI.

### 2.9.8 Supervisión basada en riesgos

Para que el auditor lleve a cabo la auditoría basada en riesgo es necesario que aplique procedimientos que estén acordes a los lineamientos establecidos por el GAFI para los entes supervisores.

Según el GAFI, los supervisores pueden considerar las siguientes categorías para evaluar los riesgos inherentes:

- Riesgo de tipo de entidad
- Riesgo del cliente
- Riesgo geográfico
- Riesgo de productos y servicios

Para controlar o mitigar estos riesgos, los supervisores pueden apoyarse de tecnologías y es aquí donde surge la importancia de la implementación de las SupTech, pues por medio de sus herramientas de análisis avanzadas, ayudan a los supervisores a mejorar su eficiencia y efectividad en la detección y mitigación de los riesgos de lavado de dinero y financiamiento al terrorismo.

Entre algunas ventajas de la implementación de SupTech por los supervisores están las detalladas en la tabla 8:

**Tabla 8**

*Ventajas de implementación de SupTech por parte de los Entes Supervisores*

| Ventaja | Descripción |
|---|---|
| Evaluación de riesgo de las entidades reguladas | La tecnología podría mejorar evaluaciones de riesgos de los supervisores de las entidades reguladas y en todo el sector. |
| Vigilancia de riesgos en todo el sistema | La tecnología podría fortalecer el riesgo general capacidades de vigilancia, apoyando la supervisión centrada en actividades para aumentar la supervisión centrada en la entidad a fin de abordar los riesgos en evolución de manera eficaz. |
| Revisiones de supervisión | La tecnología podría mejorar la eficiencia de revisiones de supervisión en el sitio / fuera del sitio al aumentar las revisiones del manual de los supervisores con análisis asistidos por máquinas de grandes conjuntos de datos |

*Nota:* Guía de Supervisión Basada en Riesgos del GAFI.

Aunque en El Salvador, la Superintendencia del Sistema Financiero aún no ha adquirido una SupTech, sí ejecuta procesos de supervisión acorde a la guía proporcionada por el GAFI, por lo que el auditor forense debe tener claro los procesos de controles y los informes que se requieren para la implementación de una supervisión basada en riesgos.

# CAPITULO III- UTILIZACIÓN DE LAS TECNOLOGÍAS SUPTECH Y REGTECH EN LAS AUDITORÍAS FORENSES CON ENFOQUE PREVENTIVO APLICADAS A EMPRESAS FINTECH QUE OPERAN EN EL ÁREA METROPOLITANA DE SAN SALVADOR

## 3.1 Generalidades

### 3.1.1 Objetivo

Establecer procedimientos que pueden ser implementados en las auditorías forenses con enfoque preventivo aplicadas a empresas FinTech pertenecientes a la vertical de pagos, apoyados en los informes generados por las Regtech; de tal manera que puedan analizarse las áreas de mayor riesgo.

### 3.1.2 Alcance

Los programas planteados a continuación están pensados para ser aplicados a empresas FinTech que pertenezcan a la vertical de pagos, que hayan contratado los servicios RegTech para ejecutar las validaciones de listas negras e identificación de operaciones inusuales y sospechosas.

Se aclara que, para efectos de este trabajo, el caso se limita al planteamiento de los programas con los cuales se evaluarán las áreas de mayor riesgo que se hayan identificado en la etapa de planificación, debiendo ser adaptados por los interesados atendiendo a la necesidad de cada auditoría.

## 3.2 Planteamiento del caso práctico - Hipotético.

La empresa (ficticia) Finnovation, S.A. es una FinTech salvadoreña perteneciente a la vertical de pagos que inició operaciones a mediados de 2020. La compañía tiene como normas de buenas prácticas adoptar controles para prevenir fraudes tomando de referencia los lineamientos que establezcan los entes reguladores y las recomendaciones emitidas por el GAFI.

Para dar cumplimiento con las regulaciones actuales y futuras, ha contratado los servicios RegTech por parte de la compañía (ficticia) RegSol, S.A. de C.V. quién tiene más de 5 años de experiencia en el campo. Dentro de los servicios que esta RegTech brinda se encuentran:

- **Debida Diligencia del Cliente:** Permite identificar si un cliente o un potencial cliente se encuentra en alguna lista negra de acceso público.

- **Monitoreo continuo de operaciones:** Da seguimiento a las operaciones en tiempo real, con lo que se facilita la detección de operaciones inusuales y sospechosas.

- **Alerta de operaciones:** Cuando el sistema detecta que una operación se sale de los parámetros normales de transacción normal de un cliente, genera una alerta para que el oficial de cumplimiento pueda darle seguimiento. Estas alertas son almacenadas y pueden ser extraídas mediante el historial de operaciones inusuales y las que se hayan catalogado como sospechosas.

Ante el incremento de nuevos usuarios, la administración de Finnovation quiere asegurarse que sus controles para prevenir fraudes están siendo efectivos, por lo que contrata al Lic. Arturo Morales; quien posee más de siete años de experiencia en la realización de encargos de auditoría forense con enfoque preventivo.

Luego de aceptar el encargo, el Lic. Arturo Morales planifica la realización del encargo que consta de las siguientes fases: (ver figura 1)

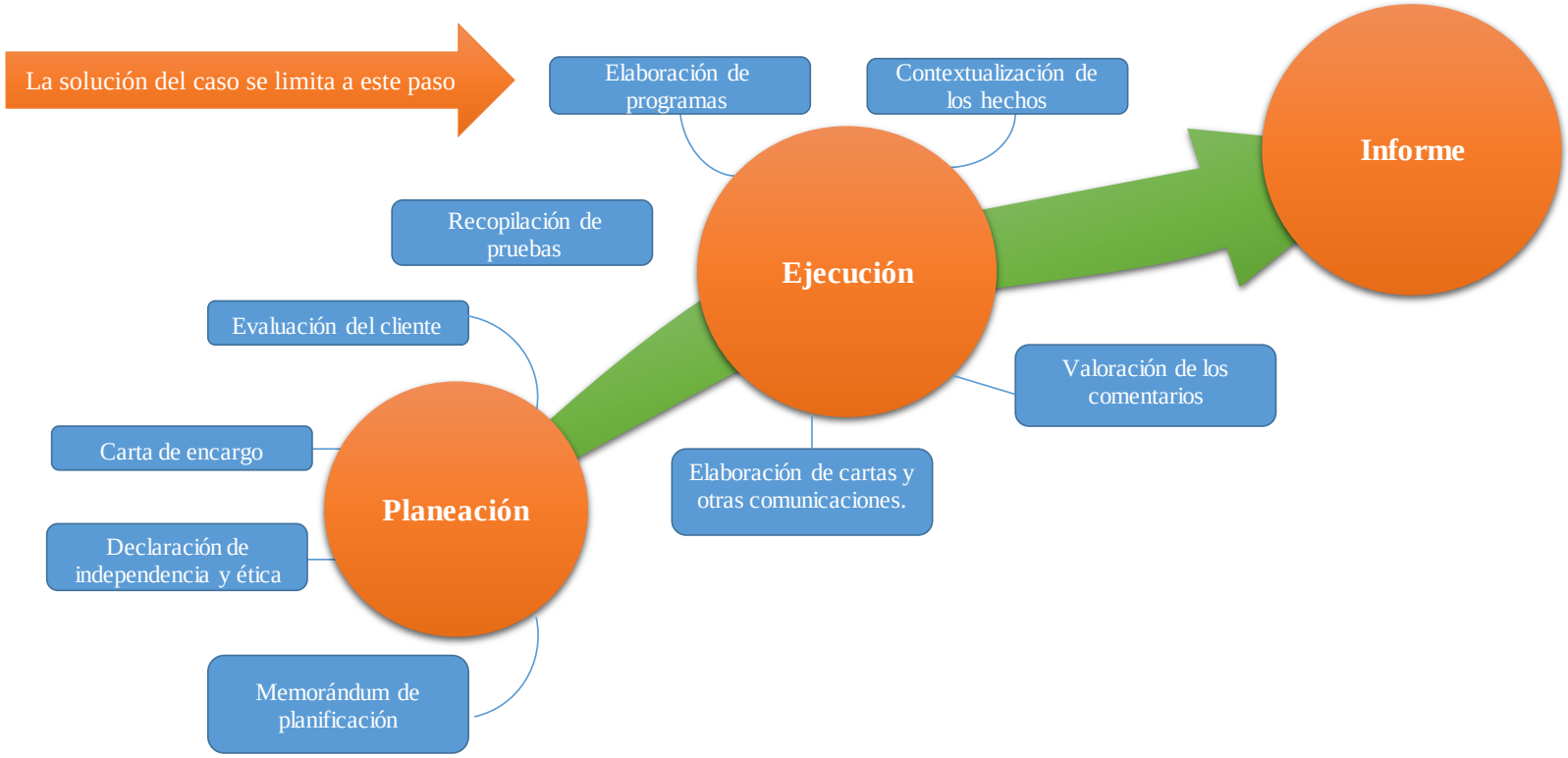



*Figura 1:* Etapas de la auditoría forense

Como resultado de la investigación de la compañía, el Lic. Arturo considera relevante los siguientes puntos:

- Finnovation funciona como una pasarela de pago, por lo que sus servicios son requeridos por comercios electrónicos que buscan ofrecer a los compradores una forma más fácil y segura de realizar los pagos.
- Para poder realizar pagos, Finnovation solicita a los usuarios vincular una tarjeta de crédito o débito, constituyendo el único instrumento de pago.
- La compañía sólo posee clientes y usuarios de nacionalidad salvadoreña.
- Con el fin de asegurar el buen manejo de la información de los usuarios, la compañía cuenta con la certificación Payment Card Industry Data Security Standard (PCI DSS),
- El único medio de acceder a los servicios es la utilización del sitio WEB y hasta el momento la administración no ha pensado en lanzar una aplicación móvil.
- El sitio WEB cuenta con la certificación Verisign parala transmisión segura de datos por Secure Sockets Layer (SSL).

Atendiendo a la información recabada sobre el funcionamiento de la compañía, el Lic. Arturo considera como principales riesgos los siguientes:

- **Riesgo de Ciberseguridad:** El sistema puede ser vulnerado y generar la pérdida de información personal de los clientes y/o suplantación de identidad de usuarios.
- **Riesgo Legal:** Al no existir una ley FinTech, pueden estarse obviando regulaciones a las que debe dar cumplimiento en atención al tipo de operación que realiza.

- **Riego de modelo:** La necesidad de recurrir a fuentes externas para facilitar el acceso a determinados datos, puede generar la pérdida de control de datos confidenciales de los clientes.

## 3.3 Programas de auditoría

Asumiendo que se han finalizado todos los pasos de la planificación, se procede a la etapa de ejecución del encargo. Para efectos de este trabajo, la ejecución se limita a la formulación de los programas de auditoría forense con enfoque preventivo.

Lo programas que se presentan a continuación, han sido creados tomando de base los supuestos contenidos en el planteamiento del caso hipotético; por lo que debe tenerse en cuenta que éstos deben ser ajustados en función de la vertical de FinTech que se quiera auditar y al conocimiento de la compañía obtenido en la etapa de planificación.

| **Nombre del Cliente:** | **Ejercicio Auditado:** | **IC** |
|---|---|---|
| Finnovation, S.A. | Al 31 de diciembre de 2021 | |
| **Programa de:** Evaluación de controles de identificación de cliente. | **Fecha:** | |

**Objetivos**

1. Verificar que la compañía cuente con controles suficientes y apropiados que le permitan tener conocimiento de sus clientes.
2. Identificar la necesidad de adoptar controles complementarios que permitan una mejor identificación de los clientes de la compañía.
3. Concluir sobre la eficiencia de los controles implementados por la entidad para el conocimiento de sus clientes.

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por y fecha | Ref P/T |
|---|---|---|---|---|
| 1 | **Políticas de aceptación de clientes**<br>Solicite la política establecida por la entidad relacionada con la aceptación de clientes, elabore una cédula que contenga una lista de chequeo para validar que la política de la compañía cumple con lo siguiente:<br>a) Que se detallen los documentos que serán requeridos al cliente para su aceptación.<br>b) Se tenga un cuestionario que permita establecer el nivel de riesgo inherente del cliente.<br>c) Que se describan las medidas de debida diligencia estándar, intensificadas y simplificadas, según el nivel de riesgo del cliente que se haya establecido.<br>d) Se describan los procedimientos a seguir para la actualización de datos de sus clientes.<br>e) Verifique que la política esté aprobada por el órgano de mayor jerarquía. | Control | | |
| 2 | **Mantenimiento de registros**<br>Evalúe el proceso de resguardo de la información mediante el diagrama de flujo elaborado por la compañia e identifique deficiencias en el control.<br><br>Solicite acceso a los medios en los cuales se posee el resguardo de los expedientes de clientes para validar que éstos sean adecuados. Los medios de resguardo pueden ser físicos y/o digitales, siempre que permitan mantener disponible la información ante cualquier solicitud de entes supervisores. | Control | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por y fecha | Ref P/T |
|---|---|---|---|---|
| | Identifique mediante la lectura de política de mantenimiento de información el plazo estipulado para su mantenimiento. Este plazo no puede ser menor a 15 años.<br><br>Elabore un cuestionario y programe una entrevista dirigida al personal a cargo del manejo de RegTech que le permita identificar:<br>a) Tipo de información que esta tecnología recopila.<br>b) Medios de almacenamiento utilizados.<br>c) Existencia de controles de seguridad de la información y forma de operar.<br>d) Personal autorizado para la extracción y manipulación de la información.<br><br>Prepare una cédula en la que vacíe los resúmenes de las respuestas obtenidas en la entrevista, luego analice la información e identifique factores que a su criterio puedan dar paso a pérdida o manipulación de información mal intencionada. | | | |
| 3 | **Procedimiento de debida diligencia.**<br>Solicite los expedientes generados por la Regtech de las personas que han sido aceptadas como clientes. Mediante el método aleatorio simple, seleccione una muestra que represente el 25% de estos expedientes.<br>Elabore una cédula que contenga una lista de chequeo que le permita validar que cada uno de los expedientes seleccionados en la muestra contiene la siguiente información:<br>a) Que se haya identificado al cliente de forma fehaciente por medio de su documento de identidad y de otra información básica que por política se solicite al momento de aceptación de cliente.<br>b) Que posea cualquier información y documentación financiera mercantil, contable, tributaria, representativa de la propiedad, posesión o tenencia de bienes muebles e inmuebles, constancia de sueldos o ingresos.<br>c) Que los expedientes de los clientes se mantengan actualizados. Para ello valide que en el expediente exista una columna que contenga la fecha de actualización. Las actualizaciones deben hacerse por lo menos una vez al año. | Control | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por y fecha | Ref P/T |
|---|---|---|---|---|
| | d) Que se hayan verificado los listados actualizados de personas naturales o jurídicas involucradas en delitos relacionados con lavado de activos, financiamiento al terrorismo y proliferación de armas de fuego. (debe cotejar con la lista actualizada publicada por países u organismos locales e internacionales vinculantes para el Estado de El Salvador).<br>e) Que se hayan verificado listados relacionados con países considerados jurisdicciones de baja o nula tributación o calificados como paraísos fiscales, personas naturales jurídicas vinculadas con actos delictivos previo a establecer o iniciar cualquier negocio con clientes potenciales y durante la continuación de la relación comercial. (debe cotejar con la lista actualizada publicada por países u organismos locales e internacionales vinculantes para el Estado de El Salvador).<br>f) Que se hayan verificado listados relacionados con personas naturales que desempeñan o han desempeñado funciones públicas destacadas en el país o el país de origen. (debe cotejar con la lista actualizada publicada por países u organismos locales e internacionales vinculantes para el Estado de El Salvador). | | | |
| 4 | **Rechazos de clientes.**<br><br>Solicite el listado de las personas que han sido rechazadas para ser parte de los clientes de la entidad, incluyendo aquellos con los que se haya decidido finalizar el contrato de prestación de servicio por detectar algún tipo de fraude y realice lo siguiente:<br><br>a) Calcule una muestra mediante el método aleatorio simple de 10 clientes rechazados y compruebe que la compañía tenga justificado el rechazo mediante la comprobación de listas negras u otro requisito que no fue cumplido por el potencial cliente y que esté contenido dentro de las políticas de aceptación de clientes.<br><br>b) Compruebe mediante copia de correo o carta de entrega (según aplique) que se hayan trasladado el listado ante la Unidad de Investigación Financiera de los clientes con los cuales se ha terminado contrato por haber detectado un posible fraude. | Control | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por y fecha | Ref P/T |
|---|---|---|---|---|
| 5 | Tomando de base los resultados de la prueba efectuada sobre las políticas y procedimientos de aceptación de clientes por parte de la compañía, concluya si la política es adecuada o si necesita ser reforzada. | Control | | |

**Elaborado por:** Auditor(a) Encargado:
**Revisado por:** Gerente de Auditoría
**Autorizado por:** Socio de Auditoría

| **Nombre del Cliente:** | **Ejercicio Auditado:** | **JC** |
|---|---|---|
| Finnovation, S.A. | Al 31 de diciembre de 2021 | |
| **Programa de:** Evaluación de los controles sobre alertas | **Fecha:** | |

**Objetivos**

**1** Verificar que la compañía cuente con controles suficientes y apropiados para la detección de señales de alerta ante esquemas de fraudes.

**2** Identificar la necesidad de reforzar los controles implementados por la entidad.

**3** Concluir sobre la efectividad o necesidad de reforzar los controles establecidos por la entidad relacionados a la detección de alertas.

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| 1 | **Procedimientos para la detección de fraudes.**<br>Solicite el manual de procedimientos que utiliza la entidad para la detección y seguimiento de alertas de fraudes. Prepare una cédula con una lista de chequeo para verificar que en ellos se establezcan los siguientes procesos:<br><br>a) Proceso para la determinación de patrones de comportamiento y transaccionalidad usual del cliente.<br>b) Procedimiento utilizado para el monitoreo de señales de alertas.<br>c) Proceso utilizado para obtener conocimiento y control de las características del mercado en el que se desarrolla la actividad económica del cliente. | Control | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | d) Proceso para la determinación de los métodos utilizados para el lavado de dinero y activos.<br>e) Programa de capacitación a los empleados sobre los instrumentos para la detección de las operaciones inusuales. | | | |
| 2 | **Monitoreo y determinación de señales de alerta** | | | |
| 2.1 | Solicite acceso a la RegTech con el acompañamiento de una persona que tenga conocimiento del funcionamiento del sistema y mediante inspección identifique lo siguiente:<br>a) Que se encuentre debidamente parametrizado en función de los factores de riesgo (clientes, productos, canales, jurisdicción y transaccional.)<br>b) Que se generen alertas en tiempo real y de manera oportuna.<br>d) Existencia de estadísticos o reportes de alertas analizadas y su respectiva calificación (normales, descartadas, inusuales, pendientes, no trabajadas).<br>e) Procedimiento para asignar, modificar o eliminar alertas del sistema. | Control | | |
| 2.2 | Solicite los estadísticos de las alertas generadas por la RegTech, y elabore un gráfico que muestre el comportamiento mensual por tipo de calificación. | Sustantiva | | |
| 2.3 | Mediante el análisis del gráfico construido, escoja 3 meses en los que existan más alertas en la calificación de pendientes y no trabajadas que estén por cumplir o tengan más de 15 días de haber sido identificadas y realice lo siguiente: | Sustantiva | | |
| | Pida al oficial de cumplimiento que brinde una explicación escrita sobre las razones por las cuales no se ha dado seguimiento a estas alertas. | Sustantiva | | |
| | Concluya si las explicaciones por las que el oficial de cumplimiento no ha dado seguimiento a las señales de alerta son satisfactorias o no. | Sustantiva | | |
| 2.4 | Selecciones 3 meses en los que se hayan detectado más operaciones inusuales. Escoja a su criterio 5 operaciones por cada uno de los meses seleccionados y realice lo siguiente: | Sustantiva | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | Solicite al oficial de cumplimiento identificar y evidenciar por medio del informe enviado a la UIF que cada operación inusual que se ha seleccionado haya sido reportada oportunamente. | Sustantiva | | |
| 3 | **CONCLUSIONES**<br>Tomando de base los procedimientos de auditoría efectuados, concluya si los controles que efectúa la entidad para la determinación de alerta de actividades sospechosas son efectivos o si es necesario que éstos sean reforzados. | Control | | |

**Elaborado por:** Auditor(a) Encargado:
**Revisado por:** Gerente de Auditoría
**Autorizado por:** Socio de Auditoría

| Nombre del Cliente: | Ejercicio Auditado: | |
|---|---|---|
| Finnovation, S.A. | Al 31 de diciembre de 2021 | **CR** |
| **Programa de:** Evaluación del cumplimiento de las regulaciones en materia de Prevención de Lavado de Dinero y Financiamiento al Terrorismo. | **Fecha:** | |

**Objetivos**

**1** Verificar que la compañía de cumplimiento a las regulaciones relacionadas con la Prevención de Lavado de Dinero y Activos.

**2** Concluir sobre el cumplimiento por parte de la entidad con las regulaciones relacionadas a la Prevención de Lavado de Dinero y Financiamiento al Terrorismo.

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| **1** | **Gestión de la Oficialía de Cumplimiento** | | | |
| **1.1** | **Estructura Organizacional de la Oficialía**<br>Solicite el organigrama de la oficialía de cumplimiento y revise que la estructura organizacional y funcional sea adecuada y esté debidamente segregada, que delimite claramente las funciones y responsabilidades, así como los niveles de dependencia e interrelación que corresponde a cada una de las áreas involucradas en la gestión del riesgo de LD/FT | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| **1.2** | **Oficialía de cumplimiento**<br>a) Verifique mediante acta que se haya nombrado al Oficial de Cumplimiento de la Institución con cargo gerencial y con suficiente autoridad e independencia para la toma de decisiones, funciones estrictamente para la prevención del LA/FT.<br>b) Que se le hayan otorgado los recursos humanos idóneos, tecnológicos y materiales para una adecuada gestión de riesgos de LD/FT para el cumplimiento de sus funciones.<br>c) Verificar mediante curriculum que el Oficial de Cumplimiento cumpla con los requisitos establecidos en el artículo 64 del Instructivo de la UIF.<br>e) Solicite la acreditación de la empresa y del Oficial de Cumplimiento ante la UIF, y que se haya comunicado oportunamente ante el ente de supervisión (15 días hábiles)<br>f) Solicite el contrato de servicio de la auditoría externa e identifique que en el alcance del contrato, se incluye revisar el área de PLA/FT | CONTROL | | |
| **1.3** | **Manual de Políticas y Procedimientos en Materia de Prevención de LA/FT** | | | |
| | Solicite el Manual de Políticas y Procedimientos y mediante lectura verifique lo siguiente:<br>a) Que esté autorizado por Junta Directiva<br>b) Que existan políticas de conocimiento al empleado, a clientes, proveedores, debida diligencia a clientes tanto simplificados como ampliados, Atención a las PPE.<br>c) Que existan Procedimiento de Consultas y Actualización de Listas de Personas de Alto Riesgo LA/FT, Procedimiento de Desvinculación de Clientes, de Análisis y Gestión de Alertas por Transacciones de Clientes y Usuarios, de Reportes ante la UIF de las Operaciones Reguladas, de Archivo y Conservación de Registros y Documentos, de Lectura de Periódicos y Actualización de Listas Negras de Personas Vinculadas con los Delitos Generadores de LAD, según Art. 6 de LCLDA, de Recepción y Remisión de los Reportes de Operaciones Inusuales (ROI), Reportes de Operaciones Sospechosas (ROS), Metodología por Factores de Riesgos (Sector supervisado por la SSF), según lo establece las Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos y Financiamiento al Terrorismo (NRP-08 del BCR), etc., | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | d) Las políticas y procedimientos deben de estar aprobados por Junta Directiva. | | | |
| | | | | |
| **1.4** | **Formularios de Vinculación y Análisis de Clientes y Empleados en Materia de Prevención de LA/FT** | | | |
| | Solicite y verifique que estén autorizados por Junta Directiva, los siguientes formularios:<br>a) Hoja Entrevista y Perfil del Cliente (KyC)<br>b) Declaración Jurada<br>c) Formulario Especial de Atención a las PPE's<br>d) Reporte Conozca a su Proveedor (KyP)<br>e) Debida Diligencia Ampliada de Clientes (DDA)<br>f) Reporte de Operaciones Inusuales (ROI)<br>g) Reportes de Operaciones Reguladas (CTR)<br>h) Conozca a su Empleado (KyE)<br>i) Reporte de Operaciones Inusuales de Empleados (ROES) | CONTROL | | |
| | | | | |
| **1.5** | **Código de Ética en Materia de Prevención de LA/FT** | | | |
| | a) Solicite el Código de Ética en materia de PLA/FT, y verifique que esté aprobado por Junta Directiva<br>b) Comprobar mediante el programa de capacitación, que sea difundido anualmente a todo el personal de la Institución<br>c) Verificar la existencia de un Comité de Ética, y si este opera para los fines que ha sido creado | CONTROL | | |
| | | | | |
| **1.6** | **Plan Anual de Trabajo y Programa de Capacitación en Materia de Prevención de LA/FT** | | | |
| | Solicite el plan anual de trabajo y el programa de capacitación de la Oficialía de Cumplimiento en materia de prevención de LA/FT y verifique lo siguiente:<br>a) Que ambos se encuentren autorizados por Junta Directiva, en el mes de diciembre o enero de cada año<br>b) Que hayan sido remitidos a los Organismos de Supervisión (SSF para supervisados) y fiscalización (UIF), en el plazo de 10 días hábiles establecido en la Ley de Supervisión y Regulación del Sistema Financiero e Instructivo de la UIF. | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | c) Que las capacitaciones incluidas en el programa de capacitación sean asignadas por áreas y temas específicos a las actividades o funciones de cada área (especializadas), y que se regule que se hará evaluación, para medir la comprensión del tema capacitado y qué hacer en los casos que alguien repruebe el examen.<br>d) Que las actividades programadas en el plan sean acordes a horas hombres con base a los días hábiles del año. | | | |
| | | | | |
| **1.7** | **Seguimiento al Plan Anual de Trabajo y Programa de Capacitación en Materia de Prevención de LA/FT** | | | |
| | Solicite el plan anual de trabajo y el programa de capacitación de la Oficialía de Cumplimiento en materia de prevención de LA/FT y constate, lo siguiente:<br>a) Que las actividades programadas tanto en el plan anual de trabajo como en el programa de capacitación, se hayan desarrollado acorde a las fechas aprobadas en dichos documentos.<br>b) Si, existen cambios o ajustes (adiciones y/o eliminaciones) a ciertas actividades programadas en el Plan Anual de Trabajo y/o Programa de Capacitación que estos estén justificados y autorizados por Junta Directiva.<br>c) Verificar que existan listas de asistencias de las capacitaciones recibidas por los miembros de Junta Directiva, Alta Gerencia y todo el personal de la Institución, evaluaciones desarrolladas con su detalle de personas que aprobaron y reprobaron el examen, cartas compromiso de haber recibido la capacitación y que lo aprendido lo pondrán en práctica en sus labores diarias.<br>d) Verificar que el personal de la Oficialía de Cumplimiento haya recibido capacitaciones en materia de Prevención de LA/FT, y que estas hayan sido especializadas, cumpliendo con lo establecido en la Ley de Supervisión y Regulación del Sistema Financiero, Ley CLDA e Instructivo de la UIF | CONTROL | | |
| | | | | |
| **1.8** | **Herramienta Tecnológica en Prevención LA/FT** | | | |
| | Confirme mediante contrato de servicio la exista de herramienta informática para el control y monitoreo de las transacciones efectuadas por los clientes y usuarios; para la prevención de los riesgos de LD/FT. | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| **1.9** | **Matriz de Riesgos en Prevención de LA/FT (Obligatorio para sociedades supervisadas por la SSF)** | | | |
| | Solicite la matriz de riesgos y verifique mediante inspección lo siguiente:<br>a) Que se evalúen e identifiquen los factores de riesgos establecidos en la NRP-08 del BCR, tales como: Clientes, Productos, Canales, Jurisdicción y Transaccional y que permita generar un nivel crediticio por cliente.<br>b) Que exista un monitoreo continuo de la matriz de riesgos | CONTROL | | |
| | | | | |
| **1.10** | **Control de Personas Políticamente Expuestas (PPE's)** | | | |
| | Solicite a la Oficialía de Cumplimiento, el listado de Personas Políticamente Expuestas (PEP´s), y verifique lo siguiente:<br>a) Que exista el formulario respectivo de Atención a PPE<br>b) Que se cuente con sistemas apropiados de gestión y consulta de riesgos para determinar si el cliente o beneficiario final es una persona políticamente Expuesta.<br>c) Que las vinculaciones de las PPE's, hayan sido aprobadas por la Alta Gerencia.<br>d) Que se haya notificado sobre las vinculación de las PPE's, en el informe trimestral al Comité de Cumplimiento y, a la Junta Directiva | CONTROL | | |
| | e) Verifique que el listado de las PPE's, esté debidamente actualizado y que se lleve a cabo un monitoreo continuo intensificado de la relación comercial . | | | |
| | | | | |
| **1.11** | **Lista de Control de Personas de Alto Riesgo LA/FT** | | | |
| | Solicite el control de Listas de Personas de Alto Riesgo LA/FT y verifique lo siguiente:<br>a) Que se encuentren debidamente actualizados.<br>b) Que estén disponibles para las áreas comerciales y de apoyo o de cualquier otra área que haga uso de dichas Listas de Cautela<br>c) Que en los casos que aparezcan coincidencias de clientes o potenciales, usuarios, prospectos o empleados, proveedores, etc., estos sean informados a la Oficialía de Cumplimiento para su análisis e investigación al respecto, a fin de determinar, si tener o no, alguna relación con dicha persona | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| **1.12** | **Respuesta a información requerida mediante oficios por parte de la UIF y Comisión Especial de Investigación, etc., de FGR y Jueces de la República.** | | | |
| | Solicite el control de oficios recibidos por la Oficialía de Cumplimiento y verifique lo siguiente:<br>a) Que este actualizado<br>b) Que se haya reportado a la persona investigada de forma oportuna en el plazo establecido en el Oficio, relativamente tiempo asignado son 10 días hábiles.<br>c) Que se haya informado al Comité de Cumplimiento y a la Junta Directiva el detalle de los oficios recibidos y remitidos; así como las coincidencias, cuando existan. | CONTROL | | |
| **1.13** | **Reportes de Operaciones Reguladas y Otros Reportes Remitidos a los entes de Supervisión y Fiscalización** | | | |
| | **1. Operaciones en Efectivo y Otros Medios**<br>Solicite que se genere del Sistema, el detalle de Operaciones individuales o múltiples realizadas con clientes o usuarios, que mediante una sola transacción diaria o la sumatoria de dos o más transacciones en el mes que hayan superaron el umbral de US$25,000 y verifique lo siguiente:<br>- Si la Oficialía de Cumplimiento las reportó a la UIF oportunamente cumpliendo con el plazo establecido en el Art. 9 de la LCLDA (5 días hábiles contados a partir del día siguiente de ocurrida la transacción o durante los primeros 5 días del mes siguiente para el caso de las operaciones múltiples o acumuladas).<br>**2. Manuales en PLA/FT y sus Modificaciones**<br>a) Investigue si han existido nuevas políticas o procedimientos o cambios a las existentes en el Manual de Políticas y Procedimientos en Materia de PLA/FT, y en el caso de existir verifique que esta(s) hayan sido informada(s) oportunamente a los Organismos de Supervisión (SSF) y Fiscalización (UIF), según lo establece el Art. 12 del Instructivo de la UIF y la Ley de Supervisión y Regulación del Sistema Financiero 10 días hábiles<br>**3. Cambios en la Designación de los Funcionarios de la Oficialía de Cumplimiento**<br>Indague con la administración si han existido cambios, y verificar lo siguiente: | SUSTANTIVA<br>CONTROL<br>CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | a) Que se haya informado a los Organismos de Supervisión y Fiscalización sobre cualquier cambio en la designación de los funcionarios de la Oficialía de Cumplimiento, indicando las razones del mismo. Así mismo, si el cambio es del Oficial de Cumplimiento, deberá adjuntarse copia legalizada del Acta de la Junta Directiva del nuevo nombramiento; acompañado del currículum vitae. (15 días contados a partir del hecho o de haberse producido el cambio) | | | |
| | **4. Reportes de Operaciones Sospechosas (ROS), Art. 9-A LCLDA y Art. 9 Disposición Especial del Instructivo de la UIF, 5 días hábiles después de su análisis para lo cual son 15 días prorrogables**<br>a) Solicite el expediente de los reportes de operaciones sospechosas.<br>b) Selecciones una muestra mediante el método aleatorio simple de 10 operaciones y verifique lo siguiente:<br>- Que hayan sido remitidos a la UIF en un plazo máximo de 5 días contados a partir del momento en que, de acuerdo al análisis que se realice, existan suficientes elementos de juicio para considerarlas irregulares, inconvenientes o que no guardan relación con el tipo de actividad económica del cliente.<br>- Que el análisis de las operaciones se haya realizado a más tardar dentro del plazo de 15 días hábiles, prorrogables una sola vez. | CONTROL | | |
| **1.14** | **Informe Trimestral al Comité de Prevención de LA/FT** | | | |
| | Confirme de su existencia mediante solicitud en requerimiento de información y verifique lo siguiente:<br>a) Que la Oficialía de Cumplimiento haya reportado por lo menos trimestralmente las actividades realizadas durante el trimestre.<br>b) Verifique mediante lectura que en las actas existan los acuerdos tomados por el Comité y que estén debidamente firmados por los miembros que participaron en dicho Comité<br>c) Verifique que los acuerdos tomados según las actas sean acordes al Reglamento del Comité aprobado por Junta Directiva, que solo traten asuntos de PLA/FT | CONTROL | | |
| **1.15** | **Informe Trimestral ante Junta Directiva** | | | |
| | Solicite el informe trimestral a la Junta Directiva y verifique lo siguiente:<br>a) Que la Oficialía de Cumplimiento reporte por lo menos trimestralmente las actividades realizadas durante el trimestre. | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | b) Solicite el libro de actas de Junta Directiva legalizado por auditor externo y verifique los acuerdos tomados y que se haya dado cumplimento de acuerdos pendientes. | | | |
| **1.16** | **Seguimiento a observaciones de los entes de Control y Supervisión (Auditoria Interna, Externa y SSF)** | | | |
| | Solicite los informes de auditorías realizadas en periodos anteriores y verifique lo siguiente:<br>a) Si existen observaciones con estatus vencidas pendientes de solventar, de las cuales solicite explicación al Oficial de Cumplimiento, a fin de documentar las causas de su estado actual.<br>b) Concluya sobre el trabajo realizado y realice los papeles de trabajo necesarios para soportar el informe de auditoría realizado. | CONTROL | | |
| **2** | **Cumplimiento de leyes, y normativas aplicables; así como políticas y procedimientos internos en materia de PLA/FT, por parte de la alta administración y todas las áreas de negocios, administrativas y de apoyo de la Institución.** | | | |
| **2.1** | **Alta Administración** | | | |
| | **Revisión de documentación e información adjunta a los expedientes de Clientes.**<br>a) Solicite o genere del sistema de clientes, el detalle de clientes activos y cancelados desde la fecha de inicio de la auditoria. Seleccione una muestra mediante el método aleatorio simple que represente el 15% de la población y verifique los expedientes contengan lo siguiente:<br>1. Expediente de identificación del cliente, según lo establece el Instructivo de la UIF<br>2. El contrato de prestación de servicios o transferencia de bienes incluye clausula en materia de Prevención de LA/FT<br>3. Perfil del cliente completado en todos sus campos<br>4. Formulario PPE, completo en todos sus campos cuando el cliente es, o ha sido PPE, según política vigente de la Compañía<br>5. Declaración Jurada debidamente completa en todos sus campos y firmada por el cliente o Representante Legal en el caso de personas jurídicas<br>6. Fotocopia de DUI del cliente, Apoderado o Representante Legal para personas jurídicas<br>7. Fotocopia de NIT del cliente, Apoderado o Representante Legal para las personas jurídicas<br>8. Fotocopia de Tarjeta de Contribuyentes IVA del cliente, en los casos que aplique | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | 9. Evidencia de que el cliente ha sido consultado en Listas de Control de Personas de Alto Riesgo LA/FT<br>10. Fotocopia de comprobante de domicilio tales como: Recibo de luz, agua, teléfono, etc.,), en el caso de personas jurídicas<br>11. Fotocopia de comprobante de domicilio, cuando en el documento de identificación oficial de la persona natural, no la describa, no sea visible o no coincida con la manifestada por el Cliente<br>12. Fotocopia de Testimonio de Escritura Pública de Constitución y sus modificaciones cuando aplique debidamente Inscrita en el CNR, en el caso de las sociedades mercantiles<br>13. Fotocopia de matrícula de comercio vigente, y en los casos que esté pendiente, la boleta de presentación en el CNR (comerciantes sociales e individuales)<br>14. Fotocopia de Acta de Constitución y Estatutos Vigentes inscritos en INSAFOCOOP o el MAG, en el caso de Asociaciones Cooperativas<br>15. Fotocopia de Acta de Constitución y Estatutos vigentes inscritos en el Ministerio de Gobernación, en el caso de las Fundaciones y ONG'S<br>16. Fotocopia de Estatutos vigentes inscritos en el Ministerio de Trabajo y Actas de Asambleas de Apoderados y Directivos, en el caso de los Sindicados<br>17. Que la documentación legal de la persona jurídica extranjera, cumple con las leyes salvadoreñas, debidamente apostillados, autenticados según sea el caso y la traducción al castellano cuando este en otro idioma<br>18. Fotocopia de Pasaporte y/o Carnet de Residencia del cliente de nacionalidad extranjera, Apoderado o Representante Legal en el caso que representen a una persona jurídica<br>19. Fotocopia de Credencial Vigente del Representante Legal, debidamente inscrita en la institución correspondiente. En los casos de estar vencida y que todavía no se haya elegido la nueva Junta Directiva, deberá de existir carta explicativa debidamente notariada<br>20. Fotocopia del Poder del Apoderado Legal y este cumple con requisitos legales, (notariado e inscrito en las entidades competentes cuando aplique)<br>21. La firma del Cliente, Representante Legal o Apoderado, consignada en la documentación del expediente coincide con la del documento legal de identificación personal. | | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | b) Verifique el proceso de consultas por parte del área de negocios de potenciales y clientes en las Listas de Personas de Alto Riesgo LA/FT<br><br>c) Verifique la existencia del control de Reportes de Operaciones Inusuales (ROI), reportados por las áreas de negocio y de apoyo a la Oficialía de Cumplimiento<br>d) Verifique si el área de negocios o de apoyo realizan procedimientos de Debida Diligencia, en cumplimiento al Art. 9B y 10 de la Ley CLDA, Recomendación 10, 12 y 22 del GAFI, Políticas Conozca a su Cliente y Debida Diligencia del Cliente, aprobadas por Junta Directiva; ya sea por iniciativa propia o por requerimiento de la Oficialía de Cumplimiento de personas de Alto Riesgo LA/FT (APNFD's, y PPE's),<br>e) Concluya sobre el trabajo realizado y realice los papeles de trabajo necesarios para soportar el informe de auditoría. | | | |
| **2.2** | **Área de Talento o Recursos Humanos** | | | |
| | a) Solicite listado de empleados activos a la fecha, seleccione muestra estadística y del resultado utilice técnica de muestreo aleatorio y con base a la política conozca a su empleado aprobada por Junta Directiva, verifique si se ha cumplido con los siguientes atributos:<br>1. Expediente de identificación del empleado<br>2. Hoja Conozca a su empleado, completo sus campos<br>3. Formulario PPE, completo en todos sus campos cuando el empleado es o ha sido PPE según política vigente de la Compañía<br>4. Fotocopia de DUI del empleado<br>5. Fotocopia de Pasaporte y/o Carnet de Residencia del empleado de nacionalidad extranjera<br>6. Fotocopia de NIT del empleado<br>7. Evidencia de que el empleado, ha sido consultado en Listas de Control de Personas de Alto Riesgo LA/FT<br>8. Fotocopia de comprobante de domicilio tales como: Recibo de luz, agua, teléfono, etc.,), cuando en el documento de identificación oficial no la describa, no sea visible o no coincida con la manifestada por el empleado<br>9. Certificación de antecedentes penales<br>10. Solvencia de la PNC<br>11. Referencias personales y laborales | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | 12. Fotocopia de atestados cuando el puesto lo requiera<br>13. Evidencia de visita domiciliar<br>14. Prueba de polígrafo cuando el puesto lo requiera<br>b) Concluya sobre el trabajo realizado y realice los papeles de trabajo necesarios para soportar el informe de auditoría. | | | |
| **2.3** | **Gerencia Administrativa o Área de Compras** | | | |
| | a) Solicite el listado de proveedores activos a la fecha, seleccione muestra estadística y del resultado utilice técnica de muestreo aleatorio y con base a la política conozca a su proveedor aprobada por Junta Directiva, verifique si se ha cumplido con los atributos siguientes:<br>1. Expediente de identificación del proveedor<br>2. Contrato de relación mercantil (cuando aplique)<br>3. Formulario Conozca a su Proveedor completo en todos sus campos<br>4. Formulario PPE, completo en todos sus campos cuando el proveedor, es o ha sido PPE, según política vigente de la Compañía<br>5. Declaración Jurada debidamente completa en todos sus campos y firmada por el proveedor o Representante Legal para personas jurídicas<br>6. Fotocopia de DUI del proveedor, Apoderado o Representante Legal para personas jurídicas<br>7. Fotocopia de Pasaporte y/o Carnet de Residencia del proveedor de nacionalidad extranjera, Apoderado o Representante Legal en el caso que representen a una persona jurídica<br>8. Fotocopia de NIT del proveedor, Apoderado o Representante Legal para las personas jurídicas<br>9. Fotocopia de Tarjeta de Contribuyentes IVA del proveedor, en los casos de que aplique<br>10. Evidencia de que el proveedor, ha sido consultado en Listas Control de Personas de Alto Riesgo LA/FT<br>11. Fotocopia de comprobante de domicilio tales como: Recibo de luz, agua, teléfono, etc.,), en el caso de personas jurídicas<br>12. Fotocopia de comprobante de domicilio, cuando en el documento de identificación oficial del proveedor persona natural, no la describa, no sea visible o no coincida con la manifestada por el proveedor | CONTROL | | |
| | 13. Fotocopia de Testimonio de Escritura Pública de Constitución y sus modificaciones cuando aplique debidamente Inscrita en el CNR, en el caso de las sociedades mercantiles | | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | 14. Fotocopia de matrícula de comercio vigente, en caso de estar pendiente, la boleta de presentación en el CNR (comerciantes sociales e individuales)<br>15. Fotocopia de Acta de Constitución y Estatutos Vigentes inscritos en INSAFOCOOP o el MAG, en el caso de Asociaciones Cooperativas<br>16. Fotocopia de Acta de Constitución y Estatutos vigentes inscritos en el Ministerio de Gobernación, en el caso de las Fundaciones y ONG'S<br>17. Que la documentación legal del proveedor persona jurídica extranjera, cumple con las leyes salvadoreñas, debidamente apostillados, autenticados según sea el caso y la traducción al castellano cuando este en otro idioma<br>18. Fotocopia de Credencial Vigente del Representante Legal, debidamente inscrita en la institución correspondiente. En los casos de estar vencida y que todavía no se haya elegido la nueva Junta Directiva, deberá de existir carta explicativa debidamente notariada<br>19. Fotocopia del Poder del Apoderado Legal y este cumple con requisitos legales, (notariado e inscrito en las entidades competentes cuando aplique)<br>20. La firma del proveedor, Representante Legal o Apoderado, consignada en la documentación del expediente coincide con la del documento legal de identificación personal.<br>21. Estados financieros, fotocopia de licencias o permisos correspondientes por las actividades que estos realizan, declaraciones tributarias y municipales juradas, etc., cuando apliquen, según política conozca a su proveedor, aprobada por Junta Directiva.<br><br>b) Consulte mediante entrevista al gerente o responsable del departamento de compras el procedimiento de debida diligencia utilizado para la aceptación de proveedores. Con esta información elabore un diagrama que le permita comprender el procedimiento ejecutado por este departamento.<br><br>c) Compare el diagrama elaborado sobre el procedimiento de Debida Diligencia ejecutado por el área de compras versus la Política Conozca a su Proveedor y Debida Diligencia del Proveedor aprobadas por Junta Directiva; ya sea por iniciativa propia o por requerimiento de la | CONTROL<br><br>CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | Oficialía de Cumplimiento e identifique posibles desviaciones.<br><br>c) Concluya sobre el trabajo realizado y realice los papeles de trabajo necesarios para soportar el informe de auditoría. | | | |

**Elaborado por:** Auditor(a) Encargado:
**Revisado por:** Gerente de Auditoría
**Autorizado por:** Socio de Auditoría

| **Nombre del Cliente:** | **Ejercicio Auditado:** | |
|---|---|---|
| Finnovation, S.A. | Al 31 de diciembre de 2021 | **EF** |
| **Programa de:** Análisis de la existencia y razonabilidad de las cifras financieras más significativas. | **Fecha:** | |

**Objetivos**

1. Verificar que los saldos financieros más significativos existen y son razonables.
2. Concluir sobre la existencia y razonabilidad de las cifras financieras más significativas.

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| **1** | **Efectivo y Equivalentes** | | | |
| 1.1 | **POLÍTICAS DE CONTABILIDAD** | | | |
| | Verifique mediante comparación que las políticas de contabilidad aplicadas a saldos en caja y bancos cumplan con la Norma International de Información Financiera para Pequeñas y Medianas Entidades (NIIF para PYMES). | CONTROL | | |
| 1.2 | **CONCILIACIONES BANCARIAS:** | | | |
| 1.2.1 | Elabore una cédula que le permita comparar los saldos según registros contables y los saldos según estados de cuentas, documentando las partidas conciliatorias. | SUSTANTIVA | | |
| 1.2.2 | Revise las actas de junta general o junta directiva y otra documentación para ver si hay evidencia de limitaciones sobre disponibilidad y uso de los saldos bancarios (incluyendo cuentas en el extranjero y saldos que se mantengan en el extranjero). | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| 1.4 | **Recálculo de Conciliación** | | | |
| 1.4.1 | Pida a la administración que solicite un estado de cuenta al 31 de diciembre de 2021 por cada banco (locales y extranjeros) con que tiene transacciones. | SUSTANTIVA | | |
| 1.4.2 | Compare los saldos finales de cada estado de cuenta con los registros contables considerando las partidas conciliatorias. | SUSTANTIVA | | |
| 1.4.3 | Haga un seguimiento de cualquier información inusual recibida en respuesta (como saldos previamente desconocidos o pasivos contingentes). | SUSTANTIVA | | |
| 1.5 | Concluya sobre la existencia y razonabilidad del Efectivo y Equivalentes al 31 de diciembre de 2021 | SUSTANTIVA | | |
| | | | | |
| 2 | Cuentas por pagar | | | |
| 2.1 | **POLÍTICAS DE CONTABILIDAD** | | | |
| | Verifique mediante comparación si las políticas de contabilidad aplicadas a las provisiones y otros pasivos están de conformidad con la Norma Internacional de Información Financiera para Pequeñas y Medianas Entidades (NIIF para PYMES) | CONTROL | | |
| 2.2 | **PROVEEDORES Y CUENTAS POR PAGAR:** | | | |
| | Obtenga el auxiliar de proveedores tanto locales como extranjeros, y compárelo con registros contables, obtenga explicaciones para cualquier diferencia resultante. | SUSTANTIVA | | |
| 2.3 | **CONFIRMACIONES A PROVEEDORES:** | | | |
| 2.3.1 | Seleccione una muestra mediante el método aleatorio simple de Proveedores tanto locales como del exterior, tomando en cuenta los saldos mayores al 15% de la Materialidad a Nivel de Cuenta, para los saldos restantes considere si es necesario efectuar una selección a juicio del auditor de acuerdo a situaciones que llamen la atención. | SUSTANTIVA | | |
| | Solicite a la administración enviar las confirmaciones de saldos al 31 de diciembre. Al recibir respuestas, cruce con los saldos contables. | SUSTANTIVA | | |
| 2.3.1 | Revise las respuestas y resúmalas como: | | | |
| | a) Saldo correcto | SUSTANTIVA | | |
| | b) Saldo incorrecto | | | |
| | c) Confirmación rechazada | | | |
| | d) Sin respuesta. | | | |
| 2.3.2 | En caso de no recibir confirmación, realice examen de pagos posteriores de los saldos seleccionados, o en su defecto la documentación que da lugar a la obligación (quedan, | SUSTANTIVA | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | comprobantes entrega de mercaderías, pagares, etc.). | | | |
| 2.4 | **RETENCIONES A EMPLEADOS** | | | |
| | Pida a la administración que solicite una solvencia y/o estado de cuenta de AFP e ISSS y en el caso de existir pagos pendientes, solicite una a la administración una explicación escrita del motivo por el cual no se ha cumplido con el pago y la fecha estimada en que se espera cumplir con la obligación. | SUSTANTIVA | | |
| | Escoja 3 meses a su criterio de los cuales debe solicitar las planillas administrativas, ISSS y AFP y mediante un cuadro comparativo, identifique diferencias entre la cantidad de personas reportadas entre la planilla ISSS versus AFP. De seguimiento a las diferencias determinadas. | | | |
| 2.5 | **IVA y Pago a Cuenta.** | | | |
| | Pida a la administración que solicite una solvencia tributaria para validar el cumplimiento del pago de los tributos. | | | |
| | Solicite las declaraciones de IVA y Pago a Cuenta del mes de diciembre incluyendo sus modificatorias y coteje el monto por pagar con los saldos registrados en las cuentas por pagar. De seguimiento a cualquier diferencia identificada. | SUSTANTIVA | | |
| 2.6 | Concluya sobre la existencia y razonabilidad de las cuentas por pagar al 31 de diciembre de 2021 | | | |
| 3 | **Capital social** | | | |
| | **POLÍTICAS DE CONTABILIDAD** | | | |
| 3.1 | Verifique que las políticas de contabilidad aplicadas al patrimonio de los accionistas cumplan con la Norma Internacional de Información Financiera para Pequeñas y Medianas Entidades (NIIF para PYMES) | CONTROL | | |
| 3.2 | **LIBROS LEGALES DE LA ENTIDAD** | | | |
| | Solicite los libros legales de la entidad: | | | |
| | - Libro de Actas de Junta General de Accionistas, | | | |
| | - Libro de Actas de Junta Directiva, | | | |
| 3.2.1 | - Libro de Registro de Accionistas, | CONTROL | | |
| | - Libro de Aumentos y Disminuciones de Capital, | | | |
| | - Libro de Estados Financieros, y | | | |
| | - Libro Diario Mayor. | | | |
| 3.2.2 | Asegúrese de que estén actualizados y que estén legalizados por el auditor externo. | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| 3.2.3 | Mediante lectura del libro de actas de Junta General identifique los acuerdos que se hayan | CONTROL | | |
| | tomado en Junta General Extraordinaria y elabore un extracto de cada uno de los acuerdos. | | | |
| 3.2.4 | Verifique que el Presidente, Secretario y/o Directores hayan firmado las actas y que en todas las juntas o asambleas haya estado presente el quórum correspondiente. | CONTROL | | |
| 3.3 | **CAPITAL EN ACCIONES** | | | |
| 3.3.1 | Verifique todos los cambios en el capital en acciones estén soportados por: | CONTROL | | |
| | - Actas | | | |
| | - Recibos de efectivo | | | |
| | - Cualquier otra evidencia. | | | |
| 3.3.2 | Compare el capital en acciones autorizado con la Escritura de Constitución de la entidad y los acuerdos tomados para cambios en la estructuración del capital. | CONTROL | | |
| 3.3.3 | Asegúrese que todos los cambios en el capital en acciones coincidan con el libro registro de accionistas. | SUSTANTIVA | | |
| 3.3.4 | Compare el capital en acciones con: | SUSTANTIVA | | |
| | - El libro mayor general | | | |
| | - Registro de accionistas y de aumento y disminuciones de capital. | | | |
| 3.3.5 | Verifique la participación accionaria de los directores con el registro legal de accionistas. | SUSTANTIVA | | |
| 3.4 | **DIVIDENDOS** | | | |
| 3.4.1 | Identifique mediante la revisión de actas de junta general ordinaria la existencia de decretación de dividendos. | SUSTANTIVA | | |
| 3.4.2 | Si se han decretado dividendos asegúrese mediante revisión de las declaraciones F-14 que se haya reportado y pagado la retención del 5% de ISR en los 10 días siguientes al mes en que hayan sido pagados los dividendos. | SUSTANTIVA | | |
| 3.4.3 | Compruebe mediante recálculo que los cálculos de los dividendos pagados sea correcto y que se haya basado en la participación accionaria de los accionistas. | SUSTANTIVA | | |
| 3.4.4 | Compare el dividendo que aparece como pagado en los estados financieros con la evidencia de pago. | SUSTANTIVA | | |
| 3.4.5 | Compruebe mediante recálculo que el cálculo de dividendos decretados pero no pagados sea correcto. | SUSTANTIVA | | |
| 3.4.6 | Concluya sobre la existencia y razonabilidad del capital al 31 de diciembre de 2021 | | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| 4 | INGRESOS | | | |
| 4.1 | **POLÍTICAS DE CONTABILIDAD**<br>Revise si las políticas de contabilidad aplicadas a los ingresos cumplen con la Norma Internacional de Información Financiera para Pequeñas y Medianas Entidades (NIIF para PYMES) | CONTROL | | |
| 4.2 | **VENTAS / INGRESOS ORDINARIOS**<br>Solicite los saldos mensuales de las cuentas de ingresos y costos de ventas.<br>Elabore una cédula que contenga los ingresos ordinarios mensuales de la compañía y analice las variaciones más significativas del período auditado. | SUSTANTIVA<br>SUSTANTIVA | | |
| 4.3 | **PRUEBA GLOBAL DE INGRESOS** | | | |
| 4.3.1 | Solicite por correo el historial de transacciones del universo de clientes y el porcentaje de comisión pactado por transacción por el período auditado. | SUSTANTIVA | | |
| 4.3.2 | Del reporte obtenido en el paso anterior calcule una muestra que incluya a aquellos clientes que mensualmente hayan realizado operaciones superiores al 25% de la materialidad por cuenta, tomando de referencia aquellos meses en los que haya identificado menores ingresos. | SUSTANTIVA | | |
| 4.3.2 | Elabore una cédula en la que recalcule la comisión cobrada de los clientes seleccionados en la muestra anterior y comparela con el cobro según el historial generado del sistema. De seguimiento a cualquier diferencia encontrada. | SUSTANTIVA | | |
| 4.3.3 | Solicite acceso al sistema de monitoreo de transacciones en tiempo real. | SUSTANTIVA | | |
| 4.3.4 | Identifique una operación que a su juicio llame la atención y de seguimiento desde su inicio hasta su incorporación en el historial de transacciones. | SUSTANTIVA | | |
| 4.3.5 | Elabore una cédula que le permita comparar las comisiones cobradas según el historial de transacción con los ingresos registrados en contabilidad. | SUSTANTIVA | | |
| 4.4 | **COMPARATIVA DE INGRESOS**<br>Solicite las declaraciones mensuales de IVA, Pago a Cuenta, Libros legales de IVA y los registros contables y compare los saldos mensuales (anexo 4 fiscal). De seguimiento a cualquier diferencia. | SUSTANTIVA | | |
| 4.5 | **INGRESOS DE INVERSIONES** | | | |
| 4.5.1 | Solicite a la administración los contratos o documentos que soporten las inversiones realizadas por la entidad. | SUSTANTIVA | | |
| 4.5.2 | Mediante lectura, identifique y proyecte los ingresos que se estima recibir durante el período auditado. Compare los resultados con el saldo | SUSTANTIVA | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | final de ingresos por inversiones reconocido durante el período para validar su razonabilidad. | | | |
| 4.6 | Concluya sobre la existencia y razonabilidad de los ingresos registrados en contabilidad. | | | |
| 5 | **GASTOS** | | | |
| | **CÉDULA PRINCIPAL (SUMARIA)** | | | |
| 5.1 | Obtenga o prepare una cédula principal (sumaria) estableciendo el resumen de gastos comparativos con el ejercicio 2021 y 2020, como se reportó en los estados financieros. | SUSTANTIVA | | |
| | **POLÍTICAS DE CONTABILIDAD** | | | |
| 5.2 | Revise si las políticas de contabilidad aplicadas a los ingresos cumplan con las Normas Internacionales de Información Financiera (NIIF para PYMES) | CONTROL | | |
| | **Gastos generales** | | | |
| 5.3 | Identifique mediante revisión de la cédula principal todos los gastos generales e identifique aquellos rubros con variaciones importantes y aquellos que durante el entendimiento de la entidad llamen la atención del auditor, obtenga respuesta de la administración respecto a las variaciones inusuales. | SUSTANTIVA | | |
| 5.4 | En los gastos que estén soportados por contrato realice una prueba global de gastos. Identifique dentro de los contratos los montos de cuotas y períodos de pago durante el ejercicio y mediante la multiplicación obtenga el gasto proyectado. Compare el resultado con los gastos según balanza. | SUSTANTIVA | | |
| 5.5 | Seleccione aquellos gastos que posean saldos más significativos con relación a la materialidad por cuenta. | SUSTANTIVA | | |
| 5.6 | De las cuentas de gastos que se hayan seleccionado en el paso anterior, solicite los movimientos por cuenta y escoja de cada uno 10 transacciones con la ayuda de la herramienta excel que permite seleccionar a los 10 mejores (montos mayores) y verifique por cada documento: | SUSTANTIVA | | |
| | • Que exista documentación de soporte | | | |
| | • Adecuado registro contable. | | | |
| | • Que el gasto corresponda a las actividades propias de la Compañía. | | | |
| 5.8 | Concluya sobre la existencia y razonabilidad de los gastos registrados en contabilidad. | | | |

**Elaborado por:** Auditor(a) Encargado:
**Revisado por:** Gerente de Auditoría
**Autorizado por:** Socio de Auditoría

| **Nombre del Cliente:** | **Ejercicio Auditado:** | |
|---|---|---|
| Finnovation, S.A. | Al 31 de diciembre de 2021 | **SG** |
| **Programa de:** Evaluación de controles de ciberseguridad | **Fecha:** | |

**Objetivos**

1. Evaluar la efectividad de los controles implementados por la entidad en materia de ciberseguridad.
2. Concluir sobre la efectividad de los controles de ciberseguridad implementados por la entidad

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| 1 | **Política** | | | |
| 1.1 | Solicite la política de seguridad de la información y verifique mediante lectura que cumple con lo siguiente:<br>a) Que esté aprobada por la alta dirección<br>b) Que esté redactada en función del propósito de la organización.<br>c) Que en ella se incluyan los objetivos de seguridad de la información o provea el marco para el establecimiento de los mismos.<br>d) Que incluya compromiso para satisfacer los requerimientos aplicables relacionados a la seguridad de información<br>e) Incluya compromiso de mejora continua del sistema de gestión de seguridad de la información. | CONTROL | | |
| | | | | |
| 1.2 | Verifique mediante revisión del plan anual de capacitación que la política de seguridad sea comunicada dentro de la organización. | | | |
| | | | | |
| 1.3 | Elabore un lista de chequeo que le permita validar que la política de seguridad de ingreso incluya como mínimo lo siguiente:<br><br>a) Requisitos de contraseña, que deben contener:<br>• Longitud mínima y máxima.<br>• Período de vigencia.<br>• Elementos permitidos ( letras, número, mezcla de mayúsculas y minúsculas, etc.)<br>• Período de actualización de contraseña. Puede estar en función del uso o tiempo.<br>• Que la actualización de la contraseña sea obligatorio.<br>• Que en las actualizaciones de contraseña no se permita usar las últimas 10 anteriores.<br>b) Intentos máximos de ingresos erróneos de contraseña. (3 intentos como máximo) | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | c) Procedimiento para recuperación de contraseñas.<br>d) Reconocimiento de las direcciones IP y que genere el aviso mediante correo del intento de inicio de cesión con IP diferente a las registradas. | | | |
| | | | | |
| 2 | **Requerimientos normativos** | | | |
| 2.1 | Compruebe mediante solicitud de certificación ISO que el sistema de gestión de seguridad de la información esté conforme con los requerimientos de la Norma Técnica ISO/IEC 27000:13. | CONTROL | | |
| | | | | |
| 2.2 | Compruebe mediante ingreso a la página WEB de Finnovation que cuente con la certificación de normas PCI estándar. Documente dicho cumplimiento mediante captura de pantalla. | | | |
| | | | | |
| 2.3 | Valide que el sitio Web es seguro mediante solicitud de certificación de seguridad informática como por ejemplo VeriSing, Systems Security Certified Practitioner, Certified in Risk and Información Systems Control, entre otras. | | | |
| | | | | |
| 3 | **Evaluación del riesgo** | | | |
| 3.1 | Solicite mediante correo el proceso de evaluación del riesgo de seguridad de la información e identifique mediante lectura que:<br><br>a) Establezca y mantenga criterios de riesgo de seguridad de la información que incluyan:<br>- El criterio de aceptación de riesgo y<br>- Criterio de desempeño de la evaluación de riesgo de seguridad de la información.<br>b) Asegúrese que repetidas evaluaciones de riesgo de seguridad de la información producen resultados consistentes, válidos y comparables.<br>c) Identifique los riesgos de seguridad de la información.<br>d) Generar una declaración de aplicabilidad que contenga los controles necesarios y a justificación para inclusiones, ya sea que sean implementadas o no, y la justificación de exclusiones de control.<br>e) Formular un plan de tratamiento de riesgo de seguridad de la información.<br>f) Obtener aprobación del plan de tratamiento del riesgo de seguridad de la información y | CONTROL | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| | aceptación de los riesgos residuales por parte de los propietarios del riesgo. | | | |
| | | | | |
| 4 | **Prueba de inicio de sesión** | | | |
| 4.1 | Intente crear una cuenta en la plataforma utilizando los datos de personas que hayan sido incluidos en listas negras y compruebe que no sea posible la creación del perfil. | SUSTANTIVA | | |
| 4.2 | Intente crear una cuenta con una contraseña que no cumpla con las condiciones que muestra la plataforma para comprobar que ésta no sea aceptada. | | | |
| 4.3 | Cree un perfil en la plataforma, posteriormente intente ingresar utilizando contraseñas diferentes a la registrada y valide que el usuario se bloquee luego de 3 intentos. | | | |
| 4.4 | Verifique en su correo vinculado que lleguen oportunamente (aproximadamente 5 minutos) la notificación de inicio de sesión que detalle el lugar aproximado y la identificación del dispositivo desde el que se está intentando iniciar sesión. Documente este procedimiento con captura del correo. | | | |
| | | | | |
| 5 | **Seguridad de base de datos** | | | |
| 5.1 | Solicite el listado del personal con privilegios especiales en los sistemas gestores de base de datos. | CONTROL | | |
| 5.2 | Detalle los privilegios que posee cada una de las personas incluidas en el listado obtenido en la instrucción anterior. Ninguno debe tener privilegios de modificar y/o eliminar logs. | CONTROL | | |
| 5.3 | Analice si los accesos de los usuarios están acorde a sus funciones. | CONTROL | | |
| 5.4 | Compruebe mediante solicitud de reporte que los gestores de bases de datos generen alarmas e informes de eventos que vulneren la seguridad. | SUSTANTIVA | | |
| 5.5 | Selecciones a criterio 3 eventos anormales que estén incluidos en el informe de eventos anormales y consulte las medidas que se implementaron para superarlos. | | | |
| 5.6 | Verifique mediante inspección los medios de almacenamiento de los logs (puede ser localmente o en repositorios externos como un servidor Syslog). | | | |
| 5.7 | Analizar si los sistemas gestores de bases de datos se encuentran bajo el perímetro de revisión de herramientas específicas de monitorización de la actividad como Guardium de IBM o Imperva. | | | |

| N° | Naturaleza y alcance de los procedimientos de auditoría | Prueba | Hecho por | Ref P/T |
|---|---|---|---|---|
| 5.8 | Solicite evidencia de la ejecución periódica sobre sistemas gestores de bases de datos, que permitan detectar vulnerabilidades ocasionadas por una deficiente configuración, existencia de usuarios in la adecuada protección, sistemas desactualizados, etc. | | | |
| | | | | |
| 6 | **Seguridad en Redes y Comunicaciones** | | | |
| 6.1 | Solicite el mapa de red del ámbito de análisis, además del mapa global para identificar los mecanismos de seguridad siguientes:<br>a) Dispositivos para el filtrado de las conexiones (firewalls)<br>b) Dispositivos para la segmentación de la red (switches)<br>c) Dispositivos de detección de intrusos y ataques.<br>d) Sistemas de análisis de correo, antivirus, proxies, etc.<br>e) Dispositivos de conexión como VPN. | CONTROL | | |
| 7 | Concluya sobre la efectividad de los controles de ciberseguridad implementados por la entidad. | | | |

**Elaborado por:** Auditor(a) Encargado:

**Revisado por:** Gerente de Auditoría

**Autorizado por:** Socio de Auditoría

# CONCLUSIONES

Como resultado de la investigación se concluye:

- Del estudio realizado se identificó que actualmente en el país se desconocen los beneficios del uso las herramientas tecnológicas RegTech y SupTech aplicadas a los encargos forenses con enfoque preventivo; sin embargo, de forma implícita muchas entidades y plataformas aplican las diferentes RegTech para el procesamiento, extracción y recopilación de información. Con la finalidad de generar mayor seguridad y transparencia en las operaciones es necesario que los profesionales de licenciatura en contaduría pública se capaciten en el uso y aplicación de las nuevas herramientas tecnológicas que ayuden a la ejecución de encargos forenses a empresas FinTech.

- Las herramientas tecnológicas en la realización de trabajos de auditoría con enfoque preventivo son cada vez más importantes e innovadoras, logrando así un alto grado de eficiencia y eficacia, ya que estas permiten verificar el cumplimiento de requerimientos regulatorios, realizar procesos automatizados, informes de calidad, supervisión en tiempo real a través de una amplia gama de tecnologías que ayudan entre otras cosas a la protección de la información obtenida a través de la supervisión y regulación tecnológica.

- Los procedimientos que se ejecuten para una auditoría forense con enfoque preventivo a una empresa FinTech deben apoyarse en las herramientas RegTech y SupTech, pues son las que se encargan de dar cumplimiento a los requisitos legales y normativos por medio de la automatización de procesos y monitoreo de operaciones que permiten prevenir, detectar y reportar los riesgos de blanqueo de capital; por lo tanto, es de vital importancia que el auditor posea la experticia necesaria para validar que los reportes generados por estas tecnologías sean adecuados.

# RECOMENDACIONES

Para utilizar las herramientas SupTech y RegTech en las auditorías forenses con enfoque preventivo a empresas Fintech se recomienda:

- Realizar investigaciones, capacitar e incentivar la inclusión de las nuevas herramientas tecnológicas que le permitan al profesional contable desarrollar trabajos de auditorías forenses con enfoques preventivos, con el objetivo de reducir el tiempo invertido en el análisis y extracción de información.

- Se recomienda a los profesionales que desarrollen encargos en auditoría forense, hacer uso de las tecnologías de supervisión y regulación tecnológica en la realización de sus procedimientos, para ello es importante que identifiquen las ventajas del uso de estas herramientas, tanto para el profesional como las empresas FinTech que auditan, siendo necesario un amplio conocimiento en el amplio tecnológico, el cual pueden adquirir a través de capacitaciones, estudios superiores o de casos de aplicación a nivel local e internacional.

- Para ejecutar una auditoría forense a una empresa FinTech con apoyo en las herramientas SupTech y RegTech es necesario que el auditor esté capacitado para la realización de una auditoría de sistemas, pues tendrá que ejecutar procedimientos que le permitan tener confianza en los procesos que éstas ejecuten para dar cumplimiento a las leyes y normativas emitidas en materia de prevención de lavado de dinero y activos.

# BIBLIOGRAFÍA

C.V, J. A. (s.f.). *JMB AUDITORES Y CONSULTORES S.A DE C.V*. Obtenido de JMB AUDITORES Y CONSULTORES S.A DE C.V: http://www.jmbauditores.com/servicios.html

Comité De Normas Del Banco Central De Reserva De El Salvador. (2013). *Normas Técnicas Para La Gestión De Los Riesgos De Lavado De Dinero y De Activos y De Financiamiento Al Terrorismo.* San Salvador.

Cuellar, C. H. (01 de 04 de 2015). *Economipedia*. Obtenido de Economipedia: https://economipedia.com/definiciones/startup.html

eID. (12 de Julio de 2021). *Electronic Identification*. Obtenido de Electronic Identification: https://www.electronicid.eu/es/blog/post/onboarding-digital-banca-sector-financiero/es

Fiscalía General de la República. (2021). *Instructivo de la Unidad de Investigación Financiera para la prevención del Lavado de Dinero y Activos.* San Salvador.

GAFI. (2020). *Activos virtuales, señales de alerta LD/FT.*

GAFI. (2021). *Supervisión basada en riesgos.*

Haddad, L. J.-V. (03 de Junio de 2011). *Revista de Contaduría Pública*. Obtenido de Revista de Contaduría Pública: https://contaduriapublica.org.mx/2010/06/03/auditor-forense/

IFAC. (2007). *Tecnología de la Información para contadores profesionales.* Nueva York.

IFAC. (2016). *Manual de Pronunciamientos Internacionales de Calidad, Auditoría,*

*Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados* (Vol. II). New York: IAASB. Recuperado el Julio de 2021

López, J. F. (03 de 05 de 2018). *Economipedia*, Fintech. (Economipedia, Productor) Obtenido de Economipedia: https://economipedia.com/definiciones/fintech.html

MAAT.AI. (21 de Abril de 2020). *MAAT.AI*. Obtenido de MAAT.AI: https://blog.maatai.com/fintech-regtech-suptech/

Security Standards Council. (2018). *Normas de seguridad de datos.*

Solis, J. J. (01 de 09 de 2017). *COBIS FInancial Stability Board*. Obtenido de COBIS FInancial Stability Board: https://blog.cobiscorp.com/que-es-regtech-clab-2017

# ANEXO

**ANEXO N°1.**

**MODELO DE GUÍA DE PREGUNTAS, ASAFINTECH.**

**UNIVERSIDAD DE EL SALVADOR.**

**FACULTAD DE CIENCIAS ECONÓMICAS.**

**ESCUELA DE CONTADURÍA PÚBLICA.**

**GUÍA DE PREGUNTAS PARA ENTREVISTA SOBRE LA "UTILIZACIÓN DE LAS TECNOLOGÍAS SUPTECH Y REGTECH EN LAS AUDITORÍAS FORENSES CON ENFOQUE PREVENTIVO APLICADAS A EMPRESAS FINTECH QUE OPERAN EN EL ÁREA METROPOLITANA DE SAN SALVADOR".**

**DIRIGIDO A:** presidente de la Asociación Salvadoreña de Tecnología Financiera (ASAFINTECH).

**OBJETIVO:** Recopilar información a fin de conocer la experiencia de los profesionales de la Asociación en el uso y manejo de las tecnologías RegTech y SupTech utilizadas a nivel local o internacional, e identificar las ventajas, desventajas y los riesgos asociados a éstas.

**INDICACIÓN:** Leer detenidamente las siguientes preguntas y conteste de la más objetiva.

**GUÍA DE PREGUNTAS.**

1. ¿Qué es FinTech y cómo funcionan?
2. ¿Considera necesario la creación de una Ley FinTech? ¿Por qué?

3. ¿Poseen las FinTech oficiales de cumplimiento?
4. ¿Considera usted que la implementación de SupTech y RegTech pueden llegar a reemplazar a los oficiales de cumplimiento?
5. ¿Conoce usted sobre casos de fraudes que se hayan detectado en el ecosistema FinTech en El Salvador?
6. ¿Qué es RegTech y cómo funcionan?
7. ¿Los datos procesados por las RegTech son totalmente manejados en la nube?
8. ¿Existen empresas salvadoreñas que presten servicios de RegTech?
9. Si no existen empresas salvadoreñas que brinden servicios de RegTech, ¿cómo hacen las empresas internacionales para adaptar sus servicios de cumplimiento a la normativa nacional?
10. ¿Cuáles son las RegTech que operan en El Salvador?
11. ¿Cuáles son las áreas en las que se aplica RegTech dentro de las FinTech que operan en El Salvador?
12. ¿Las RegTech utilizadas en nuestro país cuentan con la capacidad para adaptarse a nuevas regulaciones que pueden surgir en el futuro?
13. ¿Cuáles son los riesgos asociados en el uso de RegTech?
14. ¿De qué manera minimiza los ataques cibernéticos en las FinTech el uso de las RegTech?
15. ¿Qué es SupTech y cómo funcionan?
16. ¿La Superintendencia del Sistema Financiero utiliza la herramienta SupTech?
17. Mencione las ventajas y desventajas de cada una de las Tecnologías: FinTech, RegTech y SupTech.

18. ¿Cuáles son los riesgos asociados en el uso de SupTech?
19. ¿La inclusión del Bitcoin a la economía salvadoreña supone la necesidad de acrecentar las regulaciones y supervisiones existentes?
20. ¿Cómo pueden los supervisores fomentar la innovación y al mismo tiempo asegurar la existencia de una regulación apropiada?

**ANEXO N°2.**

**MODELO DE GUÍA DE PREGUNTAS, AUDITOR FORENSE.**

**UNIVERSIDAD DE EL SALVADOR.**

**FACULTAD DE CIENCIAS ECONÓMICAS.**

**ESCUELA DE CONTADURÍA PÚBLICA.**

**GUÍA DE PREGUNTAS PARA ENTREVISTA SOBRE LA UTILIZACIÓN DE LAS TECNOLOGÍAS SUPTECH Y REGTECH EN LAS AUDITORÍAS FORENSES CON ENFOQUE PREVENTIVO APLICADAS A EMPRESAS FINTECH QUE OPERAN EN EL ÁREA METROPOLITANA DE SAN SALVADOR.**

**Dirigido a:** Auditor Forense.

**Objetivo:** Recopilar información significativa que sirva de base para establecer ventajas e identificar los riesgos asociados a la utilización de las herramientas SupTech y RegTech en las auditorías forenses con enfoque preventivo aplicado a empresas FinTech.

**Indicación:** Leer detenidamente las siguientes preguntas y conteste de la forma más objetiva.

**GUÍA DE PREGUNTAS.**

1. ¿Qué son las RegTech y las SupTech?
2. ¿Cree usted que las herramientas RegTech y SupTech las ventajas pueden ser utilizadas para desarrollar trabajos de auditoría forense? Si_____ No____ Explique:

3. ¿Cuáles son las ventajas de utilizar las RegTech y las SupTech en una auditoría forense?
4. ¿Conoce usted alguna firma o empresa que implemente el uso de las RegTech y SupTech?
5. ¿Cómo puede el auditor utilizar RegTech y SupTech como herramientas en la auditoría forense con enfoque preventivo?
6. ¿Cuál es la normativa técnica y legal aplicable a las empresas que brindan servicios de RegTech y SupTech?
7. ¿Considera necesario que las empresas FinTech apliquen herramientas como la RegTech y SupTech? Si_____ o No____ ¿Por qué?
8. ¿Conoce usted si la Superintendencia de Sistema Financiero utiliza las SupTech como herramienta de supervisión?
9. ¿Según su experiencia cual área consideraría de mayor riesgo en una empresa FinTech? ¿Por qué?
10. ¿Considera que los riesgos inherentes en una auditoría forense con enfoque preventivo se ven reducidos si la FinTech haciendo uso de las herramientas RegTech y SupTech?
11. ¿Qué tipo de procedimientos nos facilita la utilización de las herramientas RegTech y SupTech?
12. ¿Cuáles son los conocimientos específicos que debe poseer el profesional de auditoría para realizar un encargo de auditoría forense con enfoque preventivo aplicado a una FinTech?