Universidad Andina Simón Bolívar

Sede Ecuador

Área de Gestión

Maestría en Administración de Empresas

Reorientación estratégica de una empresa de servicios de seguridad de la información orientada a prestar servicios a instituciones del sector financiero

José María Gómez de la Torre

Tutor: Sócrates Alonso Llanos Yánez

Quito, 2023

Cláusula de cesión de derecho de publicación de tesis

Yo, José María Gómez de la Torre Gómez, autor de la tesis titulada *Reorientación estratégica de una empresa de servicios de seguridad de la información orientada a prestar servicios a instituciones del sector financiero*, mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster en Administración de Empresas en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en Internet.
2. Declaro que en caso de presentarse cualquier reclamación por parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaría General, un ejemplar y sus anexos en formato digital.

Quito, 06 de mayo de 2023

Ing. José María Gómez de la Torre Gómez

Resumen

La integración de los sistemas de gestión de la calidad, seguridad y ética empresarial ha sido una plataforma para lograr una ventaja competitiva por parte de las empresas de seguridad de la información; no así en muchas empresas emergentes del Ecuador, que evidencian una escasa planificación e investigación, situación más acentuada en micro y pequeñas empresas de nuestro país. El objetivo principal de esta investigación es estudiar y reorientar estratégicamente una pequeña empresa de seguridad de la información, basándose en la combinación de los sistemas de gestión de calidad, seguridad y ética empresarial, cimentados en estándares internacionales, para la prestación de servicios de ciberseguridad a las empresas ecuatorianas del sector financiero popular y solidario. Se aborda las características principales del sector financiero desde la perspectiva de la seguridad, para lo cual se hace énfasis en la regulación y estadísticas del sector de cooperativas de ahorro y crédito, adicionalmente se analiza algunos detalles de la empresa Greenetics Soluciones, a ser analizada como caso de estudio, tales como: estructura, personal, situación financiera, mercado explotado, tamaño y servicios prestados. Se ha aplicado un método cuantitativo y cualitativo, presentando los resultados del trabajo de campo en once cooperativas de ahorro y crédito, y tres de los gremios del sector popular y solidario. Los hallazgos evidencian que las organizaciones que han logrado niveles más altos de integración son las que mayores beneficios reportan y exigen más a sus proveedores de servicio en temas de mejora continua, calidad, ética y seguridad. Más allá de estos resultados, se proponen también aspectos que podrían facilitar el proceso para futuras investigaciones, de cara a la Estructura de Alto Nivel propuesta por ISO que ayudará la integración de éstos y otros sistemas de gestión.

Finalmente, del análisis de los resultados del estudio de mercado y sobre estos resultados se plantea una reorientación estratégica que permita a Greenetics Soluciones su participación en el mercado del sector financiero de economía popular y solidaria, revelando una nueva estrategia de mejora continua basada en normativas ISO 27001 e ISO 9001, reforzada con un código de ética y alianzas estratégicas.

A Dios, Padre Celestial, supremo creador del universo y de nuestro pequeño planeta azul, que me ha permitido estar en este instante de la vida del mundo, que me ama con amor eterno y que me ha facultado el ver en cada ser humano mi propio rostro; al todo poderoso que gobierna: a cada átomo y destello de energía de mi ser, a cada emoción de mi alma y a cada fragmento de mi espíritu.

A los docentes académicos y los compañeros de la Universidad Andina Simón Bolívar, quienes compartieron conmigo no solo conocimientos, pero también su amistad invaluable y gratos momentos de compañerismo.

A mi tutor de tesis Alonso Llanos por su apoyo, entereza, acertada dirección y consejos oportunos.

A mi esposa Vicky, hijos José María, Andrés, Emilio y Anahí, mis hermanos Blanca y Nacho, mis demás familiares, mis compañeros de trabajo y mis amigos en general, por la paciencia que han tenido mientras desarrollo esta tesis de grado.

Tabla de contenidos

Introducción

Problema de investigación

Greenetics Soluciones S.A. como empresa de seguridad informática, tiene la necesidad de proponer nuevos servicios de ciberseguridad a los potenciales clientes del sistema financiero, con innovación, manteniendo estándares de calidad y resguardando la información entregada, buscando ganar y mantener su confianza.

Dentro del sector financiero se han identificado dos segmentos de mercado a ser explotados, estos son el segmento bancario y el segmento de cooperativas de ahorro y crédito. Según la Superintendencia de Bancos (SB 2018), en abril de 2018 operan en el Ecuador 23 instituciones bancarias privadas, en tanto que la Superintendencia de Economía Popular y Solidaria constan cinco segmentos con un total de 64 cooperativas de ahorro y crédito de los segmentos 1 y 2 (SEPS 2017).

Para los análisis que se realizarán en este trabajo se ha considerado los años 2015, 2016 y 2017, debido a que es el período en el que ha funcionado la empresa Greenetics objeto del estudio. Adicionalmente en este período se ha promulgado la regulación de seguridad de la información que actualmente está vigente, el 05 de marzo de 2015 la Superintendencia de Economía Popular y Solidaria (SEPS 2015) y el 02 de septiembre de 2014 la Superintendencia de Bancos (SB 2014).

Las instituciones del sector financiero contratan los servicios de ciberseguridad con empresas independientes a la entidad, dotadas de personal capacitado y con experiencia (SB 2014, 13), situación que al momento aún resulta difícil de acreditar dentro del sector financiero, por parte del personal de la empresa Greenetics Soluciones S.A.

Actualmente la empresa Greenetics Soluciones S.A. no cuenta con una estrategia que le permita iniciar y mantener acuerdos de cooperación conforme a los sugerido por Fred David, cuando afirma que las alianzas estratégicas y los acuerdos de cooperación se utilizan cada vez más, porque permiten a las empresas mejorar las comunicaciones y el establecimiento de redes, globalizar las operaciones y reducir al mínimo los riesgos (2008, 177); esto con la finalidad específica de lograr superar la brecha de capacitación y experiencia de su personal, que como resultado le faculte

competir exitosamente en las licitaciones de servicios de ciberseguridad en el sector financiero.

Como consecuencia de las limitaciones mencionadas, hasta la presente fecha la empresa Greenetics Soluciones S.A. ha participado en 8 licitaciones públicas de requerimientos de servicios de seguridad de la información en bancos y cooperativas, logrando obtener un solo resultado favorable.

Objetivo general

Plantear una reorientación estratégica de la empresa de servicios de seguridad de la información Greenetics, incorporando una filosofía empresarial de mejora continua, una metodología de seguridad de la información interna, indicadores de gestión y un código de ética empresarial; considerando que, para poder alcanzar su principal mercado objetivo, que es el sector financiero de cooperativas del Ecuador, tiene la necesidad de lograr alianzas estratégicas o acuerdos de cooperación.

Objetivos específicos

Analizar pormenorizadamente la estructura organizacional de la empresa Greenetics Soluciones S.A. para identificar las medidas que se deben adoptar para su reorientación estratégica.

Analizar el estado de la seguridad de la información en el sector financiero de cooperativas de ahorro y crédito del Ecuador, conforme a un muestreo significativo, en un nivel de representatividad superior al 50% respecto de los activos, y determinar las mejoras que pueden ser aplicadas. Segmentos 1 y 2.

Investigar las filosofías de mejoramiento continuo, para elegir la que mejor se ajuste a una empresa de seguridad de la información, conforme a un análisis investigativo de otras empresas de similar operación, para ser utilizada como base para cimentar la reorientación estratégica de una empresa de servicios de seguridad de la información.

Conocer los estándares de seguridad de la información, para elegir y estudiar el que mejor se ajuste a la reorientación estratégica de la empresa Greenetics, considerando los más aplicables para este tipo de empresas.

Describir la influencia que el ecosistema empresarial puede tener en una empresa de seguridad de la información como Greenetics, al implementar una metodología de seguridad de la información y un código de ética empresarial.

Desarrollar un marco teórico que permita orientar y enfocar sobre cómo se debe realizar el estudio y evitar errores, permitiendo contar con un fundamento técnico para explicar los análisis y resultados del estudio.

Justificación práctica

En el Ecuador existen 6 asociaciones de Cooperativas de Ahorro y Crédito, que apoyan la Investigación de nicho de mercado, la cual servirá para que la empresa Greenetics Soluciones S.A. mejore su estrategia y estructura empresarial, a fin de que pueda lograr el estándar exigido para calificar en los procesos de contratación de seguridad de la información de las empresas del sector financiero y demás empresas privadas y públicas que requieran servicios de ciberseguridad.

También ayudará indirectamente a fortalecer la imagen y percepción de confianza de la empresa Greenetics y de cualquier otra empresa de seguridad de la información que añada a su estrategia la filosofía de mejora continua, la seguridad de la información y la ética empresarial.

Justificación teórica.

Como punto de partida se realizará un diagnóstico estratégico de la empresa Greenetics Soluciones S.A. lo que involucrará un análisis del adentro y afuera de la organización, así como la elaboración de una matriz de las amenazas, oportunidades, debilidades y fortalezas. (David 2008, 234)

Con base a los resultados del diagnóstico estratégico se procederá a determinar la estrategia que será implementada, basándose en dos pilares fundamentales que son el mejoramiento continuo de la gestión de calidad (Prieto 2011, 5) y la implementación de la seguridad de la información (Prieto 2005, 8).

Del benchmarking realizado, se ha elegido a las dos principales empresas de seguridad de la información de los países vecinos, Colombia y Perú, estas son: Digiware y Securesoft, respectivamente; mismas que se perfilan como rivales, ya que han incursionado con fuerza en el mercado de seguridad de la información del sector

financiero del Ecuador; de lo investigado, estas empresas han considerado en su estrategia la incorporación de una filosofía de mejora continua y un modelo de seguridad de la información, como ejes importantes para el sector.

Para el mejoramiento continuo y la gestión de la calidad se analizará la posibilidad de utilizar una filosofía empresarial, tales como: “Kaizen”, “Lean”, “Total Quality Management”, “Six Sigma”, siendo la optimización de los procesos y la incorporación de indicadores de gestión la base principal para la reorientación estratégica de la empresa Greenetics. Los resultados de la investigación de gestión de calidad en las empresas ecuatorianas demuestran un impacto favorable de éstas en la calidad de sus procesos y productos y, por lo tanto, en la satisfacción de sus clientes. (Benzaquen y Pérez 2016, 168)

Para la decisión de la filosofía de mejoramiento continuo es importante considerar y analizar que el gobierno de Japón mantiene un plan de asistencia Kaizen para los países en desarrollo del sudeste Asiático, América Latina y Europa del este (Ohno 2009, 1), a diferencia de otras metodologías de mejoramiento continuo tales como “Six Sigma”, “Lean” o “Total Quality Management” a las cuales se puede acceder únicamente contratando consultores internacionales que representarán un costo adicional, difícil de pagar para una MIPyME, como lo es la empresa Greenetics Soluciones S.A.

Para la implementación de la seguridad de la información se considerarán tres metodologías: ISO 27000, AICPA SOC 2 e ITIL, que luego del análisis respectivo preliminar, se determina que el estándar ISO 27000 es reconocido en el país como norma de aplicación nacional (INEN ISO 27000), y la mayor parte de los sectores económicos del Ecuador basan muchos de sus procesos en viarias normas ISO, 9000 para la calidad, 14000 para gestión ambiental, 20000 calidad de los servicios de TI y 27000 seguridad de la información (SB 2014, 11) (SEPS 2015, 2).

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un sistema de gestión de seguridad de la información es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones (ISO 270001 en español, 3).

Capítulo primero
Marco Teórico

El marco teórico que guiará el presente trabajo de investigación comprende los conceptos y definiciones respecto de: los modelos de seguridad de la información, modelos de gestión de calidad y de reorientación estratégica; con el propósito de facilitar al lector la comprensión del análisis qué se pretende realizar en los capítulos siguientes.

1 Análisis de tres modelos de seguridad de la información

Según Watkins (2008, 13) se tiene por definición de seguridad de la información a la preservación de la confidencialidad, la integridad, la disponibilidad, principalmente, así como también de la autenticidad, responsabilidad, no repudio y confiabilidad de la información. También complementa esta definición indicando que no es solo la información la que nos tiene que preocupar, sino también el almacenamiento, manejo, movimiento y procesamiento de ésta; al considerar todas estas previsiones citadas, es relativamente fácil concluir que cada organización debería preocuparse por sus compromisos de seguridad de la información de manera particular.

A continuación, vamos a describir tres de los principales modelos de seguridad de la información utilizados mundialmente, que son el SOC 2, ISO 27001 e ITIL.

1.1 Modelo de seguridad SOC 2 de AICPA

AICPA es el instituto americano de auditores, que cuenta con tres marcos de trabajo *(frameworks*) SOC 1, SOC 2 y SOC 3, como modelos de seguridad para controles de sistemas y organización, que en sus siglas en ingles significa: System and Organization Controls (SOC), ("AICPA - American Institute of CPAs" 2018).

El modelo SOC 1 cuenta con los compromisos que informan sobre la efectividad de los controles internos en una organización de servicios que pueden ser relevantes para el control interno de los informes financieros (SCIIF) de sus clientes.

El modelo SOC 2 evalúa controles internos, políticas y procedimientos, que se relacionan directamente con la seguridad de un sistema, en una organización de servicio. El modelo SOC 2 se diseñó para determinar si las organizaciones de servicio cumplen con los principios de seguridad, disponibilidad, integridad de procesamiento, confidencialidad y privacidad, también conocidos como los principios de los servicios de confianza. Estos principios abordan los controles internos no relacionados con el SCIIF.

El modelo SOC 3, al igual que el modelo SOC 2, se basa en los principios de los servicios de confianza, pero hay una gran diferencia entre estos dos modelos, que es el uso restringido del informe de auditoría. Un informe de SOC 3 puede distribuirse libremente, mientras que un informe de SOC 1 o SOC 2 solo puede ser leído por las organizaciones usuarias que dependen de sus servicios. El modelo SOC 3 puede proporcionar a las partes interesadas el informe del auditor sobre si una entidad mantuvo controles efectivos sobre sus sistemas, sin proporcionar una descripción del sistema de la organización de servicio.

Para determinar el modelo de seguridad, SOC 1, SOC 2 o SOC 3 se ha considerado los siguientes cuestionamientos:

¿Los servicios de seguridad de la información prestados por Greenetics, podrían causar modificaciones directas a los informes financieros de un cliente? La respuesta es no, por lo que la metodología SOC 1 no sería la aplicable.

¿Greenetics desea ser evaluada en los Principios del Servicio de Confianza? Sí, motivo por el cual los modelos SOC 2 y SOC 3 deben ser considerados.

¿El uso restringido afecta su decisión? Sí afectan la decisión, por lo que considerando que los modelos SOC 1 y SOC 2 solo pueden ser leídos por las organizaciones de usuarios que dependen de sus servicios. Un modelo de SOC 3 puede distribuirse libremente y usarse en muchas aplicaciones diferentes, por lo que no es el tipo de modelo que se necesita.

Luego de haber planteado las preguntas clave, el tipo de modelo de seguridad que se precisa es el de tipo SOC 2.

Un factor importante en la implementación de SOC 2 es que se debe considerar que, en cada uno de estos modelos, los informes deben ser emitidos por una firma de Auditoría, CPA[1] con licencia.

Los servicios requeridos por el sector financiero son de altísima confianza, por lo que SOC 2 introduce una lista de criterios en cuatro áreas: Políticas, Comunicaciones, Procedimientos y Monitoreo. En cada área se evalúan los cinco principios considerados por AICPA para la seguridad de la información, que son:

• Seguridad: el sistema está protegido contra el acceso no autorizado (tanto físico como lógico).

• Disponibilidad: el sistema está utilizable para su funcionamiento y uso según lo comprometido o acordado.

• Procesamiento de integridad: el procesamiento del sistema es completo, preciso, oportuno y autorizado.

• Confidencialidad: la información designada como confidencial está protegida según lo comprometido o acordado.

• Privacidad: la información personal se recopila, utiliza, retiene, divulga y destruye de conformidad con los compromisos en el aviso de privacidad de la entidad y con los criterios establecidos en los Principios de Privacidad Generalmente Aceptados (GAPP) emitidos por AICPA (AICPA 2012, 18).

El informe de auditoría en la metodología SOC 2 está diseñado para asegurar que los riesgos relacionados con los procesos subcontratados a una organización de servicios se aborden mediante controles efectivos.

Para abordar el riesgo alto, algunas entidades financieras requieren descripciones de control muy detalladas y elaboradas, mientras que otras entidades financieras pueden estar satisfechas con menos. Determinar el nivel apropiado de detalle puede ser un desafío para Greenetics, por lo que es importante que la entidad financiera establezca una relación y comunique sus necesidades y expectativas de seguridad de la información.

Las entidades financieras deben verificar que las organizaciones de servicio de seguridad de la información proporcionen un informe completo de metodología SOC

[1] Contador Público Autorizado. Definición tomada de < http://www.ccpp.org.ec/> Consulta realizada en septiembre de 2018.

2 y procurar esforzarse para establecer una relación de beneficio mutuo, donde se pueda determinar los requisitos de cada organización.

Algunas organizaciones de servicios de seguridad de la información pueden no entender cómo un modelo de SOC 2 puede ayudar a su negocio, por lo que pueden ser reacios a invertir sus recursos económicos y humanos en la obtención de uno. Sin embargo, se puede mencionar que una clara ventaja es la mejora de la competitividad que obtienen, al aplicar mejores prácticas de seguridad de la información cuando implementan e informan sobre sus controles.

Una organización de servicio de seguridad de la información, que no adopta la metodología SOC 2 en favor de sus usuarios financieros, eventualmente se encontrará en una desventaja competitiva significativa frente a las demás, que si han adoptado una metodología SOC 2.

La privacidad, la disponibilidad y la confidencialidad de los datos son preocupaciones cada vez mayores para las empresas que recopilan y procesan ciertos tipos de datos, a medida que los reguladores ajustan las reglas sobre la gobernanza de datos. Es más probable que las entidades financieras que se preocupan por la integridad, la confidencialidad y la privacidad se asocien con organizaciones de servicios auditadas por una firma independiente, que pueda proporcionar un informe sobre la metodología SOC 2.

Además, las entidades financieras que se preocupan por la disponibilidad y la integridad del procesamiento, están más inclinadas a asociarse con organizaciones de servicio que pueden proporcionar un informe SOC 2 sobre sus controles operacionales. La mayoría de las empresas del sector financiero están utilizando sistemas de TI para realizar sus operaciones críticas; necesitan asegurarse de que sus organizaciones de servicio tengan procedimientos y controles establecidos para proporcionar servicios confiables (AICPA 2012, 34).

1.2 Sistemas de gestión de seguridad de la información ISO 27001

La norma ISO 27001 es parte de la familia de normas ISO / IEC 27000, que es un conjunto de estándares realizados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), centrados en ayudar a las organizaciones a mantener seguros los activos de información de sus empresas, ya sean estas grandes o pequeñas.

Las normas ISO 27000 permiten a las organizaciones administrar la seguridad de activos tales como: información financiera, propiedad intelectual, detalles de los empleados o información que le haya sido confiada por terceros ("ISO/IEC 27001 Information security management" 2018).

La familia de normas ISO 27000 consta de 39 normas, de manera particular para el sector financiero. Se pondrá énfasis en tres de ellas la ISO 27001, ISO 27002 e ISO 27015.

La norma ISO 27001, también es una norma nacional aprobada por el INEN con el nombre: NTE INEN-ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información – requisitos; esta es una norma certificable como empresa y/o como proceso, para garantizar la seguridad de la información en una empresa (INEN 2017a, 1).

La norma ISO 27002, que también consta como norma nacional con el nombre: NTE INEN-ISO/IEC 27002:2013 Código de práctica para los controles de seguridad de la información, establece las directrices para la seguridad de la información en las organizaciones, así como las prácticas de gestión de seguridad de la información incluyendo: la selección, la implementación y la gestión de los controles; todo esto siempre teniendo en consideración el entorno de riesgos de seguridad de la información de la organización que la está adoptando (INEN 2017b, 1).

La norma ISO 27015 tiene como nombre: Directrices de gestión de seguridad de la información para los servicios financieros, también ha sido adoptada por el INEN como normativa nacional; esta tiene la particularidad de complementarse y sumarse a los controles de seguridad de la información definidos en la norma ISO 27002, para iniciar, implementar, mantener y mejorar la seguridad de la información dentro de las organizaciones que prestan servicios financieros (INEN 2016a, 1).

Uno de los principales objetivos de la ISO 27001 es alinearse al propósito del negocio, cubriendo el eje de seguridad de la información, independientemente del tamaño de la empresa o industria; esto se lo consigue con la implementación de un Sistema Gestor de Seguridad de la Información, sus siglas SGSI, cuyo principal propósito es disminuir la posibilidad de ocurrencia de un incidente de seguridad de la información, y en caso de que el incidente acontezca, permitir la minimización del impacto en la operación de la empresa.

El Sistema Gestor de Seguridad de la Información SGSI permite a una empresa o industria, el mejoramiento de la postura de seguridad digital, una mayor claridad en la inversión en seguridad de la información, un aumento de la credibilidad dentro de su segmento de acción, así como la gestión del riesgo desde la perspectiva de la seguridad de la información.

La norma ISO 27001 es una norma técnica, que no solo se aplica a los procesos de las empresas de tecnología, sino también a los activos y procesos tecnológicos relacionados al núcleo de cualquier tipo de negocio, de cualquier empresa o industria; de esta manera se podrán considerar enfoques diferentes, de acuerdo con el giro del negocio, para lograr los procedimientos seguros y obligatorios para todas las actividades de gestión de la seguridad de la información. (INEN 2017a, 2)

la norma ISO 27001 considera dentro de la planificación de la seguridad de la información, la necesidad de definir dónde se encuentra la responsabilidad de seguridad de la información dentro de la organización, para que los comités y los órganos de revisión estén en un lugar administrativamente adecuado para cumplir y satisfacer los requerimientos del Sistema Gestor de Seguridad de la Información SGSI.

Se define por parte de Watkins (2008, 31) que los recursos humanos necesarios para llevar a cabo las tareas relacionadas a la seguridad de la información, también deben considerarse y gestionarse de manera adecuada. Esto incluye considerar los acuerdos de aprovisionamiento, verificación, administración y salida del personal, así también al personal de los contratistas y cualquier otra persona que interactúe con la empresa dentro del alcance de su SGSI; esto incluye a cualquier persona que tenga acceso físico a las instalaciones, desde y hacia las cuales se pueda acceder a los activos relacionados con la información.

La norma ISO 27001 exige que los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes de seguridad de la información, sus responsabilidades y compromisos, también asegura que estén equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal y para reducir el riesgo.

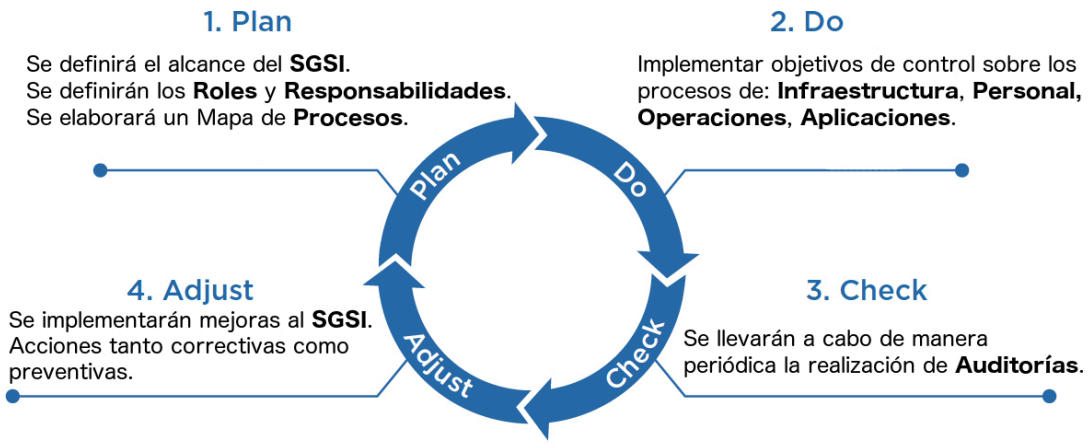
Según Williams (2013, 46) se debe proporcionar un nivel adecuado de conocimiento, educación y capacitación a todos los empleados, contratistas y usuarios de terceros, en procedimientos de seguridad y uso correcto de las instalaciones, así como en el procesamiento de la información, todo esto enfocado a minimizar los

posibles riesgos de seguridad. Se debe establecer un proceso disciplinario formal para manejar infracciones de seguridad.

La norma ISO 27001 adopta el modelo "Planificar, Hacer, Verificar, Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI, según se puede apreciar en el gráfico 1, en el que se ilustra cómo un sistema de gestión de seguridad de la información, SGSI toma como entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen con esos requisitos y expectativas.

Gráfico 1

Modelo PHVA utilizado en la Norma ISO 27001



Fuente: (“ISO/IEC 27001 Information security management” 2018)

Elaboración propia

El Sistema Gestor de Seguridad de la Información SGSI permite a las organizaciones demostrar el grado de madurez de seguridad con respecto a sus prácticas de seguridad de la información, lo cual es muy aplicable y necesario en un sector tan crítico como el financiero popular y solidario.

Para Watkins(2008, 39), la integridad del SGSI permite a los clientes (en este caso del sector financiero) confiar en la certificación, en lugar de insistir en enviar a sus propios auditores para proporcionar las garantías requeridas por sus propios directores, partes interesadas y clientes. Esto permite ahorrar mucho tiempo, costos e interrupciones; tanto para la empresa prestadora del servicio, como para la auditoría y las partes auditadas, es un beneficio que contribuye a la aceptación de la certificación acreditada por ISO27001 sin mayor reparo.

Por otro lado (Calder y Watkins 2008, 21–22) comentan los beneficios de adoptar un sistema de gestión de seguridad de la información externamente certificable:

- Los directores de la organización podrán demostrar que cumplen con las mejores prácticas internacionales actuales en gestión de riesgos con respecto a los activos de información y seguridad.
- La organización podrá demostrar, en el contexto de la variedad de legislación pertinente, que ha tomado las medidas adecuadas para cumplir con las leyes, en particular (GDPR) el Reglamento de Protección de Datos de la UE.
- La organización podrá protegerse sistemáticamente de los peligros y costos potenciales del mal uso de la computadora, el cibercrimen y los impactos de la ciberguerra.
- La organización podrá mejorar su credibilidad con el personal, los clientes y las organizaciones asociadas; esta credibilidad mejorada puede tener beneficios financieros directos a través, por ejemplo, de mejores ventas.
- La organización podrá tomar decisiones informadas y prácticas sobre qué tecnologías y soluciones de seguridad desplegar, para aumentar la rentabilidad de la seguridad de la información; gestionar y controlar los costes de la seguridad de la información, permite medir y mejorar su rentabilidad, así como sus inversiones en seguridad de la información.

1.3 Information Technology Infrastructure Library - ITIL

ITIL es una biblioteca de infraestructura de tecnologías de la información, que se define como la implementación y gestión de servicios de tecnologías de la información-TI de calidad, que satisfacen las necesidades del negocio. Los servicios de TI son proporcionados por proveedores de tecnologías de la información (la entidad que brinda servicios de TI a clientes internos y externos) a través de una combinación adecuada de personas, procesos y tecnología de la información (Kaiser 2017, 2).

Muchas de las técnicas para satisfacer la calidad o mejorar los tiempos de atención del área de informática, fueron desarrolladas y aprendidas desde el Centro de Datos, o más conocido por su nombre en inglés, Data Center; estas técnicas permanentemente se aplican y se mejoran hacia nuevos desafíos, ya que también se

requieren algunos nuevos e importantes conceptos como la seguridad y las medidas a ser tomadas frente a desastres. Durante varios de los últimos años, la comunidad de personas de tecnologías de la información que piensan críticamente sobre la gestión de la capacidad computacional, ha comenzado a compartir mejores prácticas entre sí, y esas mejores prácticas han encontrado su camino en el conjunto de todas las mejores prácticas operacionales de TI, conocidas como la Biblioteca de Infraestructura de TI o ITIL.

Actualmente la biblioteca ITIL consta de seis libros. El primer libro es una introducción al área completa de la gestión de servicios de TI, y los otros cinco libros forman el núcleo de las recomendaciones de mejores prácticas. ITIL es un conjunto de recomendaciones basadas en miles de ejemplos y decenas de años de experiencia de muchos contribuyentes. Debido a toda esa experiencia y el gran escrutinio que han recibido las recomendaciones, ninguna debe tomarse a la ligera. Por otro lado, es bastante probable que ninguno de los contribuidores haya trabajado en un situación exacta, por lo que no podría prever todos los matices y desafíos que enfrentará al implementar la administración de capacidad o cualquier otra disciplina de ITIL (Klosterboer 2011, 4).

ITIL se compone de procesos, o sea un conjunto estructurado de actividades diseñadas para lograr un objetivo específico, cada proceso en ITIL toma una o más entradas y las convierte en salidas definidas. Todos los procesos son medibles, entregan resultados esperados, dan servicio a los clientes y responden a requerimientos o necesidades específicas.

Hay veintiséis procesos y cuatro funciones en ITIL, los procesos no se ejecutan solos, necesitan personas para llevar a cabo las actividades individuales del proceso y las personas que buscan los procesos provienen de las funciones. Para decirlo simplemente, las funciones proporcionan los recursos necesarios para que los procesos completen sus objetivos (Kaiser 2017, 13).

Dentro de la organización financiera, hay verticales, por ejemplo, el núcleo bancario, la venta minorista y el seguro. Existen procesos que afectan a todas las verticales de la organización, como los recursos humanos. Las personas en las verticales desempeñan su papel en el proceso de recursos humanos, que es el corte horizontal en todas las verticales, a pesar de que son parte de una función. Este sería un ejemplo de cómo un proceso aprovecha las funciones para llevar a cabo los objetivos establecidos.

La implementación de la administración de la capacidad de ITIL es compleja y costosa, por lo que antes de dar inicio es importante tener los objetivos previamente definidos, ya que la implementación no es suficiente para explicar el retorno de la inversión, por lo que se necesita definir metas muy específicas y mensurables para la organización.

El diseño de la capacidad tecnológica es fundamental para diseñar cualquier clase de servicio, conocer qué tan grande y cuánto se va a necesitar para la gestión de la capacidad. El volumen de diseño del servicio también describe los otros elementos clave que forman parte del diseño de un servicio de TI, como la gestión del nivel de servicio y la gestión de la seguridad de la información.

La gestión de la seguridad de la información es un proceso que se ocupa de la seguridad de los datos, especialmente los datos del cliente; es importante tener en cuenta que uno de los aspectos que proporcionan garantía de servicio es la seguridad de la información. Si esta garantía de seguridad falla, entonces la parte de utilidad de un servicio deja de tener sentido, lo que daña íntegramente el objetivo del servicio. En efecto, la gestión de la seguridad es uno de los procesos más importantes dentro del ciclo de vida del servicio ITIL.

En ITIL la gestión de seguridad de la información es un proceso de gobernanza, que garantiza que los riesgos que surgen de la perspectiva de la seguridad de la información se identifiquen y se manejen de manera adecuada, luego se gestionen todos los aspectos de la seguridad de TI, ya sean: datos de aplicaciones, información empresarial confidencial o la seguridad del centro de datos.

En el ciclo de vida de un servicio en ITIL, una política de seguridad de la información proporciona las reglas y los límites necesarios para garantizar el cumplimiento de los objetivos de gestión de la seguridad de la información. La alta gerencia debe respaldar completamente las pautas de la política y garantizar que haya comunicación suficiente con el resto de la organización; las políticas no cubren solo al proveedor del servicio, sino que también abarcan a los clientes.

Según la publicación de Kaiser (2017, 88) para el diseño de servicios de ITIL, éstas son algunas de las políticas que conforman la política de seguridad de la información:

- Una política general de seguridad de la información
- Uso y mal uso de la política de activos de TI

- Una política de control de acceso
- Una política de control de contraseña
- Una política de correo electrónico
- Una política de Internet
- Una política de antivirus
- Una política de clasificación de la información
- Una política de clasificación de documentos
- Una política de acceso remoto
- Una política con respecto al acceso del proveedor al servicio, información y componentes de TI
- Una política de infracción de derechos de autor para material electrónico
- Una política de disposición de activos
- Una política de retención de registros

De acuerdo con las mejores prácticas de ITIL, la administración de seguridad de la información existe para mantener protegida la información del cliente, los datos, los activos y todos los aspectos de los recursos del cliente. Si vemos hacia el cliente, de seguro este tendrá ciertas políticas y pautas establecidas para la seguridad del negocio.

El objetivo de la administración de la seguridad de la información es alinearse con la seguridad del negocio del cliente y garantizar que la empresa se mantenga intacta, de acuerdo con los principios de seguridad de la información: 1. Confidencialidad: solo se puede acceder a la información por aquellos que están autorizados. 2. Integridad: la información es precisa, completa y está en una condición textual. 3. Disponibilidad: la información está disponible cuando sea necesario para aquellos quienes están autorizados. 4. Autenticidad: las transacciones entre varias partes (empresa a empresa o empresa a proveedor y otras relaciones) son confiables.

1.4 Comparación modelos de seguridad de la información

Del análisis realizado a los tres modelos de seguridad de la información, SOC2, ISO 27001 e ITIL, en la tabla 1 se tiene un cuadro de análisis comparativo, que nos facilitará la toma de decisión, para la reorientación estratégica de la empresa Greenetics Soluciones S.A.

Tabla 1

Comparación modelos de seguridad de la información

	AICPA SOC 2	ISO 27001	ITIL
Tipo de framework	Mejores prácticas	Estándar	Mejores prácticas
Símil Ecuador	No se tiene	INEN ISO 27001	No se tiene
Gestión de Riesgo	Sí	Sí	No
Certificable	Sí	Sí	No (ISO 20000)
Considera un Plan de continuidad del negocio	Opcional	Sí	Sí
Incluye métricas y controles	Sí	Sí	Sí
Áreas	7 ejes de acción	10 dominios	26 procesos y 4 funciones
Creador	AICPA	ISO International Organization for Standardization	OGC
¿Para qué se implementa?	Auditoría de Sistemas de Información	Cumplimiento del estándar de seguridad	Gestión de Niveles de Servicio
¿Quiénes lo evalúan?	Compañías de contabilidad Compañías de consultoría en IT	Compañías de Consultoría en IT, Empresas de Seguridad Consultores de seguridad en redes	Compañías de Consultoría en IT

Fuente: ISO 27001, AICPA SOC 2 y ITIL

Elaboración propia

Se realizó una tabulación de las certificaciones publicadas por las empresas de seguridad de la información que operan en el Ecuador y las que constan registradas en el Centro de Ciberseguridad Industrial CCI de España, obteniéndose los resultados que se muestran en la tabla 2.

Tabla 2

Cantidad de empresas de seguridad de la información

	AICPA SOC 2	ISO 27001	ITIL
SOC según CCI	0/21	14/21	9/21
CERT según CCI	0/11	9/11	5/11
Operan en Ecuador	0/5	3/5	1/5

Fuente: (“Home - Centro de Ciberseguridad Industrial” 2018), FIRST

Elaboración propia

2 Análisis de modelos de gestión de calidad

2.1 Kaizen

La metodología Kaizen se ha desarrollado gradualmente durante muchas décadas. Fue públicamente y oficialmente presentado al mundo en la década de 1980 como una metodología de mejora continua de la calidad sistemática, a través del libro más vendido Kaizen, por Masaaki Imai, el fundador del Instituto Kaizen (“Kaizen Institute Consulting Group” 2018).

Kaizen es una filosofía, se define como el espíritu de la innovación basada en el espíritu de la cooperación y sinergia, que se desarrolla paralelamente en todos los niveles: de la vida personal, la casa, social y en el trabajo (Brunet 2003, 8).

La aplicación específica de Kaizen en el trabajo significa la mejora continua de todos los días, en todo momento, de todas las personas, desde la directiva, pasando por las gerencias, hasta los trabajadores en general (Imai 2012, 28).

La implementación de Kaizen involucra a todos los que forman parte de la empresa y requiere una permanente sujeción a sus principios. No requiere ser implementada como un proceso, sino vivida intensamente como una filosofía. Para lograr esto la gerencia debe reunir los elementos y sistemas principales de la empresa para establecer la estrategia Kaizen que incluya: el ciclo planear, hacer, revisar y actuar, procesos frente a resultados, la calidad siempre primero, hablar con datos y el principio de que siempre el siguiente paso es el cliente (Imai 2012, 25).

Kaizen consolida la participación en equipos de trabajo, incrementando el potencial de aprendizaje y conduciendo a un mejor entendimiento del cambio y la cooperación en el lugar de trabajo, sin embargo, se dificulta romper la barrera cultural al ser un modelo japonés (Brunet, 2003).

Si la administración tiene éxito en el mejoramiento de la cultura de la organización, la compañía será más productiva, más competitiva y más lucrativa a largo plazo; sin embargo, todo el impacto del esfuerzo que la administración hace para mejorar la cultura no se sentirá sino hasta años después. Si los gerentes están interesados principalmente con las utilidades inmediatas, estarán renuentes a dedicar tiempo y esfuerzo en el mejoramiento de la cultura, y con el tiempo puede la organización llegar a ser más competitiva (Imai 1989, 269).

Los principios del Kaizen permiten llevar al personal a un nivel de compromiso no solo con sus actividades asignadas, sino a un involucramiento integral con el accionar de la empresa, pasando del pensamiento y la emotividad a la acción y mejora continua (Lareau 2003, 52-55).

Kaizen ha sido implementado en todos los países del mundo, no depende del idioma o el nivel de educación de su fuerza laboral, este puede ser entendido por los presidentes de las compañías, así como por los trabajadores de los niveles más básicos. Adicionalmente considera todas las ideas buenas, y el trabajo fuerte no solo beneficia a la compañía sino a cada uno de los trabajadores haciendo su trabajo más sencillo, donde todos ganan (Geoffrey 2006, 27).

Desarrollar una ventaja estratégica para enfrentar la competencia es uno de los mayores logros de la gerencia de una compañía y de sus ejecutivos, la competitividad significa garantizar la supervivencia hoy en día en los mercados globalizados, todo esto dependerá en qué tan bien la planificación Kaizen ha sido desarrollada (García Oropesa Maldonado 2000, 131-132).

2.2 ISO 9001

La familia de normas ISO 9000 se creó, en su forma inicial, en 1987, y experimentó revisiones sustanciales en 1994, 2000 y 2008. La última versión de la norma se lanzó en 2015, misma que se encuentra vigente actualmente. A nivel mundial, estas normas se extendieron en su fase inicial a lo largo de los países de la Unión Europea UE, especialmente relevante en el Reino Unido, lo cual es

perfectamente lógico en vista de la experiencia previa de ese país con la BS 5750, que fue base para la ISO 9001 (Heras-Saizarbitoria 2018, 1–2).

ISO 9001 es un estándar internacional certificable, que establece los requisitos para un Sistema de Gestión de Calidad SGC. Ayuda a las empresas y organizaciones a ser más eficientes y mejorar la satisfacción del cliente. Los requisitos de este estándar son genéricos, se aplican a cualquier sector, área de negocio y pueden implementarse en cualquier organización, independientemente de su tamaño o el tipo de sus productos o servicios ("ISO 9001 Quality management" 2018).

ISO 9001 la cual ya ha sido adoptada por el INEN como norma nacional con el identificativo NTE INEN-ISO/IEC 9001:2015 Sistemas de gestión de la calidad – requisitos, esta es una norma de calidad certificable como empresa y/o como proceso empresarial (INEN 2016b, 1).

La aplicación del estándar ISO 9001 permite a una organización demostrar su capacidad de proporcionar consistentemente productos o servicios que cumplan con los requisitos reglamentarios, para mejorar la satisfacción del cliente mediante el uso de instrumentos de gestión de calidad, que incluyen métodos para planificar y mejorar procesos, garantizar la conformidad con los requisitos reglamentarios y legales del cliente (Abuhav 2017, 1).

En la versión del año 2015 la norma ISO 9001 está estructurada en siete elementos principales: (a) contexto de la organización, (b) liderazgo, (c) planificación, (d) apoyo, (e) operación, (f) evaluación del desempeño y (g) mejora (INEN 2016b, 2).

En caso de surgir preguntas o malentendidos sobre las definiciones o los requisitos de la Norma ISO 9001 durante la implementación y aplicación de los requisitos estándar, se puede consultar el documento "ISO 9000: 2015: Sistemas de gestión de calidad: Fundamentos y vocabulario". Por ejemplo, cuando está discutiendo y planificando actividades relacionadas con el enfoque al cliente y no está seguro de cuál es la definición de enfoque al cliente, puede recurrir al Estándar ISO 9000 y comprender cómo el Estándar ISO 9001 debe interpretar el tema de atención al cliente (Abuhav 2017, 3).

La versión actual, ISO 9001: 2015, se esfuerza por hacer que sea un importante impulsor en el modelo comercial de la organización. ISO 9001:2015 agrega requisitos para que la organización demuestre la integración de los requisitos del Sistema Gestor de Calidad SGC, en sus procesos comerciales y también para proporcionar un análisis de riesgos que respalde el cumplimiento de los objetivos de calidad. Adicionalmente

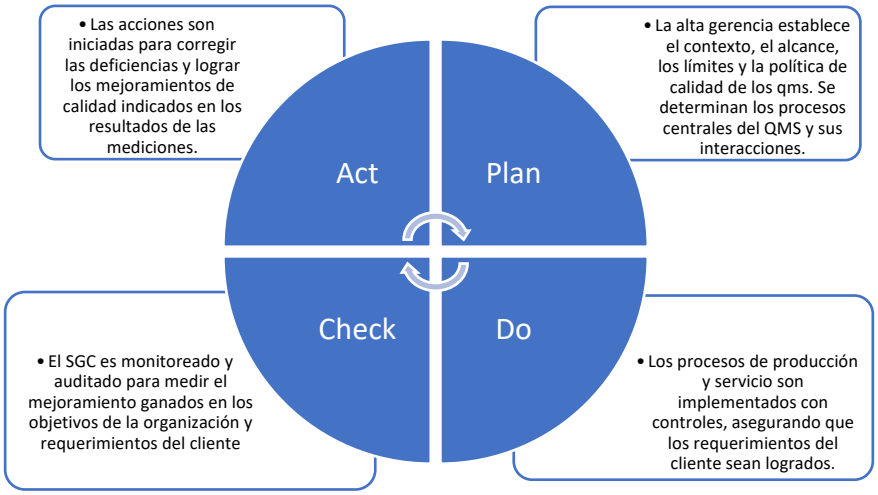
requiere que las organizaciones consideren los problemas externos y las partes interesadas que son relevantes para el Sistema Gestor de Calidad SGC, aparte de los clientes tradicionales, proveedores y empleados. Los problemas externos que podrían afectar la estrategia comercial de la organización, como la nueva tecnología, las posibles fuerzas del mercado y la competencia, están abiertos a la auditoría en el esquema ISO 9001:2015 (Dentch 2017, 6).

La definición del contexto de la organización comenzará con el análisis PEST (factores políticos, económicos, sociales y tecnológicos), que proporcionará insumos para el análisis de fortalezas, debilidades, oportunidades y amenazas (FODA). El análisis FODA definirá las entradas para la determinación de los problemas internos y externos, La determinación de los problemas internos y externos ayudará a identificar a las partes interesadas pertinentes. Identificar a las partes interesadas ayudará a definir el alcance del SGC, que finalmente proporcionará la base del SGC (Abuhav 2017, 9).

El estándar internacionalmente reconocido para la gestión de calidad ISO se basa en el enfoque PDCA plan-do-check-act. Este es el principio de funcionamiento de todos los estándares de sistemas de gestión ISO, incluida ISO 27001 para gestión de seguridad de la información (Dentch 2017, 7).

Gráfico 2

Modelo PHVA utilizado en la Norma ISO 9001



Fuente: (“ISO 9001 Quality management” 2018)

Elaboración propia

El Estándar requiere el cumplimiento de todos los requisitos mencionados en la norma, cuando sean aplicables, en otras palabras, no puede excluir ni descuidar ningún requisito de la norma a menos que este requisito no sea aplicable a su SGC y

que tenga una justificación aceptable. Por ejemplo, si no se está comprando ningún servicio o producto de un proveedor externo, no tiene sentido el desarrollar herramientas y controles de gestión de calidad para esas áreas (Abuhav 2017, 35).

La implementación de este tipo de norma es voluntaria, aunque en ciertos sectores su aplicación constituye una obligación de facto o por regulación sectorial. La motivación de las empresas para obtener la certificación muchas veces viene conducida por las grandes empresas, de sectores como el de la construcción, automoción, energía y telecomunicaciones. Este último vio en la norma ISO 9001 una forma de garantizar un cierto nivel de calidad por parte de sus proveedores y subcontratistas, en el sentido de obtener una cierta sistematización y formalización de los procesos clave utilizados por dichas empresas, para cumplir con los requisitos que las grandes empresas establecieron, pero sin aumentar sus costos operacionales (Heras-Saizarbitoria 2018, 3).

2.3 Gestión de Calidad Total - TQM

La gestión de la calidad total, en Inglés por sus siglas TQM (Total Quality Management) plantea que toda empresa tiene como objetivo mantenerse en el mercado, para satisfacer las necesidades de sus clientes, impulsando la estabilidad de la colectividad, ofreciendo satisfacción y progreso a los integrantes de la organización.

Uno de los mejores ejemplos de calidad en la producción en empresas industriales es Toyota, a quien la mayor parte de autores citan como caso de éxito, ya que ha sabido conjugar valores y principios de calidad total, tales como la eficiencia de recursos, la velocidad y la flexibilidad de producción.

Con el avance industrial vino el fortalecimiento del desarrollo de TQM y la calidad fue controlada a través de habilidades supervisadas, descripción escrita, medición y estandarización. Durante la Segunda Guerra Mundial, los sistemas de fabricación se volvieron complejos y la calidad comenzó a verificarse mediante inspecciones externa, en lugar de los propios trabajadores (Dahlgaard, Khanji, y Kristensen 2007, 7).

Es importante saber que la gestión de calidad total, TQM es un término muy popular, sin embargo, muchas veces se queda en palabras muy rimbombantes, pero sin ningún efecto práctico, es por esto por lo que actualmente y para efectos del presente análisis se ha considerado TQM, con la variante de Lean Six Sigma.

El término Lean, en español nos indica esbeltez, ya que nos sugiere la identificación y eliminación de desechos en los procesos involucrados en la producción, es decir mantener el ambiente de trabajo y sus procesos de la manera más sencilla y simple, dentro de la complejidad que un ambiente de trabajo puede significar.

A cada producto o servicio se le agrega valor como resultado de un proceso, la adición de valor ocurre en todas las etapas del proceso, el valor del producto implica la disposición del cliente a pagarlo, el cliente requiere cada producto con valor máximo a bajo costo. Los residuos implican una actividad que el cliente no está dispuesto a pagar, el desperdicio es para una industria o empresa, lo que consume recursos, tiempo, pero que no mejora el valor del producto, ni genera valor en ningún sentido (Antony, Vinodh, y Gijo 2016, 24).

Lean es una filosofía que se basa en el desarrollo de productos de la más alta calidad con el menor costo y entrega a tiempo. Dentro de la filosofía de la calidad, la producción Lean se centra en minimizar los pasos donde se producen los derroches, así como en mejorar la velocidad de fabricación. Los principios Lean aseguran un historial establecido de éxito operacional y estratégico, lo que facilita mayor valor para el cliente.

Respecto de los cinco principios o valores del sistema de producción Lean, Antony, Vinodh y Gijo (2016, 25) coinciden en que la preferencia percibida por el cliente se sustenta en la evaluación de las características del producto, para favorecer el logro de sus objetivos, esto es el precio más bajo, con la mayor cantidad, mejor calidad y menor tiempo de entrega; indican que el flujo de valor basado en los requisitos del cliente no deben tener ningún obstáculo, esto sin cuellos de botella en el proceso que permita el flujo de valores; se centra en la producción basada exclusivamente en los requisitos del cliente, minimizando y eliminando en lo posible el inventario. La mejora continua implica un perfeccionamiento gradual de productos, procesos o servicios a lo largo del tiempo, con el objetivo de reducir los residuos para mejorar la funcionalidad del lugar de trabajo, el servicio al cliente o el rendimiento del producto, la política de gestión a largo plazo debe implementarse para implementar la empresa Lean.

Six Sigma tiene al menos tres significados, según el contexto. En primer lugar, se puede ver como una medida de calidad, ya que Sigma es una letra griega que mide la variación en un proceso, donde lograr una medida de calidad seis (Six) Sigma

significa que los procesos están produciendo menos de cuatro defectos por millón de eventos. En segundo lugar, Six Sigma se puede ver como una estrategia de mejora empresarial y una filosofía. En tercer lugar, es una metodología de resolución de problemas que busca encontrar y eliminar las causas de los defectos o errores en los procesos comerciales, al centrarse en los resultados del proceso que son críticos a los ojos de los clientes (Antony, Vinodh, y Gijo 2016, 27).

Los autores Antony, Vinodh y Gijo (2016, 30) describen de manera general, la metodología de resolución de problemas Six Sigma, utilizando una potente metodología de cinco etapas, basada en datos para mejorar los procesos. Las cinco etapas de la metodología Six Sigma son:

Definir: en esta etapa, uno tiene que definir el problema y el proceso al que está asociado el problema. Se decidirán los objetivos e hitos del proyecto y se definirán los requisitos del cliente, tanto interno como externo.

Medir: en esta etapa, se debe medir el rendimiento del proceso en estudio. El objetivo principal de esta etapa es recopilar datos válidos y confiables pertinentes al alcance del proyecto.

Analizar: en esta etapa, uno tiene que determinar las causas del bajo rendimiento o la variación excesiva que conducen a defectos o errores en el proceso en estudio. Se pueden usar varias herramientas estadísticas para analizar los datos y determinar la posible causa raíz del problema.

Mejorar: en esta etapa, uno tiene que desarrollar soluciones potenciales que puedan mejorar el rendimiento del proceso y reducir el impacto del problema en cuestión.

Controlar: El propósito de esta etapa es mantener el rendimiento optimizado, generar un plan detallado de monitoreo de soluciones, observar las mejoras implementadas para tener éxito, actualizar los registros del plan de manera regular y mantener una rutina de capacitación laboral viable.

Se puede tener Gestión de Cambio sin mejora continua; sin embargo, no se puede tener Mejora Continua sin la Gestión del Cambio. Es un requisito en cada etapa de un proyecto Lean Six Sigma, y sin el reconocimiento de su importancia y el despliegue a lo largo de todo el proyecto, no tendrá éxito. (Kesterson 2018, 3)

Six Sigma permite a las organizaciones mejorar sus procesos, haciéndolos capaces de ofrecer lo que el cliente quiere, desde la primera vez de la relación comercial. Según comentan Antony, Vinodh y Gijo (2016, 31), aquellas

organizaciones que implementan Six Sigma correctamente, logran beneficios significativos que contribuyen a la ventaja competitiva y a cambiar la cultura en una organización, desde la resolución de problemas reactivos hasta la prevención proactiva. Los siguientes son algunos de los beneficios potenciales de Six Sigma:

• Mayores ingresos: Six Sigma aumenta los ingresos al permitir a su organización hacer más con menos (es decir, debería poder producir más productos o brindar más servicios con menos recursos).

• Costos operacionales reducidos: Six Sigma reduce los costos asociados con el desecho, reelaboración, reparación, reemplazo, garantía, tiempo de inactividad, etc.

• Mejora de la moral de los empleados: Six Sigma puede mejorar la moral de los empleados al involucrarlos en el proceso de mejora. Desarrolla un sentido de propiedad y responsabilidad para sus empleados.

• Reducción de siniestros: el uso efectivo de Six Sigma puede reducir los costos asociados con los esfuerzos de resolución de problemas mal dirigidos o la lucha contra desastres.

• Habilidades mejoradas para la resolución de problemas: Six Sigma utiliza un conjunto de herramientas dentro de la metodología de resolución de problemas, y las personas que están involucradas con el proyecto Six Sigma tendrán la oportunidad de aprender cómo las herramientas trabajan en la solución de problemas del mundo real.

• Comunicación mejorada: Six Sigma exige trabajo en equipo, la comunicación entre los miembros del equipo puede mejorarse, además, la comunicación entre los miembros del equipo y el equipo directivo superior también mejorará significativamente a partir de diversas intervenciones y mediante reuniones periódicas de revisión de la gestión de los proyectos.

• Mayor calidad y confiabilidad: la metodología Six Sigma se puede utilizar para reducir las tasas de defectos e incluso prevenir defectos en los procesos. Esto llevaría a una mayor calidad y confiabilidad del producto.

2.4 Comparación modelos de gestión de calidad

Del análisis realizado a los tres modelos de gestión de la calidad, TQM, Kaizen e ISO 9001, se tiene en la tabla 3 un cuadro comparativo, que nos facilitará la toma de decisión, para la reorientación estratégica de la empresa Greenetics.

Tabla 3

Comparación modelos de gestión de calidad

	Kaizen	ISO 9001	TQM
Tipo de framework	Estándar	Estándar	Estándar
Símil Ecuador	No se tiene	INEN ISO 9001	No se tiene
Gestión de Riesgo	Sí	Sí	No
Certificable	Sí (internacional)	Sí (local)	Sí (internacional)
Considera un Plan de continuidad del negocio	Sí	Sí	No
Incluye métricas y controles	Sí	Sí	Sí

Fuente: Kaizen, ISO 991 y TQM

Elaboración propia

Se realizó una tabulación de las certificaciones de las empresas de seguridad que operan en Ecuador y las que registra en el Centro de Ciberseguridad Industrial CCI de España, obteniéndose los resultados mostrados en la tabla 4.

Tabla 4

Cantidad de empresas de Gestión de Calidad

	Kaizen	ISO 9001	TQM
SOC según CCI	0/21	9/21	0/21
CERT según CCI	0/11	5/11	0/11
Operan en Ecuador	0/5	4/5	0/5

Fuente: (“Home - Centro de Ciberseguridad Industrial” 2018), FIRST

Elaboración propia

3 Reorientación estratégica

3.1 Matriz de Perfil Competitivo, MPC

Es la clasificación de fortalezas y debilidades específicas, que permite identificar a los principales competidores de una empresa, para lo cual se incluyen factores internos y externos (David 2008, 112).

3.2 Matriz de Evaluación del Factor Externo, EFE

Es la que estructuralmente facilita al momento de construir una estrategia, ya que nos da la posibilidad de consolidar y analizar en una vista los datos de tipo: económicos, culturales, sociales, demográficos, ambientales, legales, políticos, gubernamentales, tecnológicos y competitivos (David 2008, 110).

Que un evento neutral sea una oportunidad o amenaza para una empresa determinada, depende de dos factores principales. El primer factor es la capacidad de la empresa para reconocer el evento. Si el evento es significativo y pasa desapercibido, hay posibilidades de que el evento represente una amenaza de supervivencia para la empresa no informada. El segundo factor es la capacidad de la empresa para reaccionar de manera positiva al evento en sí. La capacidad de reaccionar de manera positiva depende por completo de la capacidad de la empresa para aplicar los recursos necesarios que transformarán un evento ambiental neutral en una oportunidad para la empresa (Van Deusen, Williamson, y Babson 2007, 62).

3.3 Matriz de Evaluación del Factor Interno, EFI

La matriz de evaluación del factor interno es la que muestra las fortalezas y las debilidades más importantes de una empresa, de una manera colectiva, calificada y ponderada; para elaborar la EFI es adecuado iniciar con una auditoria o evaluación interna, dentro de ésta se procede a la reunión y utilización de los datos sobre: gerencia, marketing, negocios, contabilidad, fabricación, operaciones, exploración y desarrollo (David 2008, 121).

3.4 Matriz de Amenazas, Oportunidades, Debilidades y Fortalezas

El análisis de fortalezas, debilidades, oportunidades y amenazas, también conocido como análisis FODA, se usa ampliamente en el mundo académico y empresarial para comparar y contrastar organizaciones. La herramienta abarca las fortalezas y debilidades, que son los atributos internos de los elementos comparados, pero también las características externas que pueden agregarse a sus fortalezas y debilidades, para convertirse en estrategias (Kumar y Phrommathed 2005, 15).

La matriz de fortalezas, oportunidades, debilidades y amenazas (FODA) es un instrumento de administración de empresas, para ayudar a los directivos a establecer cuatro prototipos de estrategias: estrategia ofensiva con la correlación de fortalezas y oportunidades (FO), estrategias de reorientación con la interrelación entre debilidades y oportunidades (DO), estrategias defensivas con la conexión entre fortalezas y amenazas (FA) y estrategias de supervivencia con la correspondencia entre debilidades y amenazas (DA). El ajuste entre los factores internos y externos es la parte más difícil de desarrollar en una matriz FODA y requiere un criterio acertado (David 2008, 200).

3.5 Estrategias específicas y objetivos a largo plazo

Los objetivos a largo plazo significan en términos de efectividad, en los resultados esperados por aplicar estrategias específicas definidas y asociadas a estos objetivos estratégicos. Las estrategias contienen entre otras cosas, las tácticas y las acciones que se llevarán a cabo para lograr cumplir las metas de los objetivos a largo plazo. Normalmente se considera un periodo de dos a cinco años, como un tiempo adecuado para lograr conformar la relación entre los objetivos y las estrategias (David 2008, 158).

3.6 Indicadores

Son las mediciones o puntos de control que ayudan a la organización a conocer si los problemas de la empresa se deben a incongruencias en la estrategia, o a afirmar

la estrategia adoptada, en función de las metas logradas en el cumplimiento de los objetivos trazados con la estrategia (David 2008, 302).

Capítulo segundo
Descripción del caso de estudio

1 Descripción de la empresa Greenetics Soluciones S.A.

De las visitas realizadas a la empresa Greenetics Soluciones S.A., entre los meses de marzo a julio de 2018, se han podido efectuar seis entrevistas a los principales ejecutivos de la empresa, donde se ha logrado levantar la información necesaria para poder realizar la descripción de la empresa.

Greenetics Soluciones S.A. es una empresa de sociedad anónima, del tipo micro, pequeña y mediana empresa (MIPyME), enfocada en brindar soluciones para seguridad informática, que cuenta con experiencia técnica en el área de Ciberseguridad, ofreciendo productos y servicios para protección contra amenazas informáticas, pérdida de datos, robo de información, suplantación de identidad, análisis forense informático, capacitación especializada, outsourcing de seguridad y atención de incidentes de seguridad de la información.

La empresa Greenetics Soluciones S.A. frente a sus clientes asume la responsabilidad integral de supervisar y mantener la seguridad de la información, los clientes pertenecen a diversos sectores de la sociedad, pero se pretende enfocar el accionar de la empresa hacia el sector financiero popular y solidario.

1.1 Filosofía empresarial

Actualmente Greenetics no cuenta con una filosofía empresarial definida, tampoco ha desarrollado una estrategia empresarial como tal; sin embargo, se puede mencionar que de manera informal tiene algún tipo de estrategia, para brindar soluciones tecnológicas en ciberseguridad, para el desarrollo de sus clientes, proporcionando herramientas para la operación segura y continua de sus sistemas.

1.2 Estructura organizacional

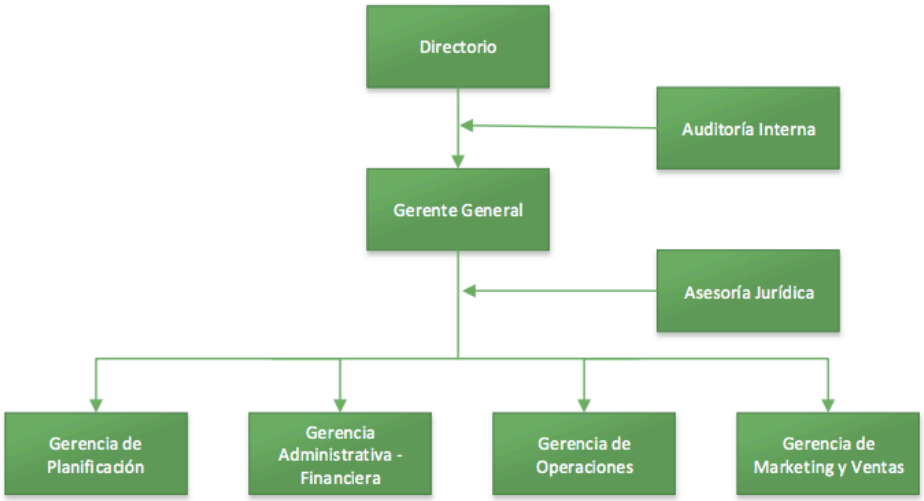
En lo que tiene que ver con la estructura organizacional, se pudo conocer que es un emprendimiento de 4 años de formación, que aún mantiene algunas de las estructuras y formas de trabajo que vienen desarrollando desde su constitución el 17 de julio de 2014, en este sentido se ha podido levantar la siguiente información:

Las decisiones de más trascendencia para la empresa derivan de la junta directiva, que está conformada por los cuatro socios que conforman la empresa, para lo que teóricamente se programan dos reuniones mensuales, pero supieron indicar que en la realidad manejan una razón de dos reuniones trimestrales, de las cuales se genera un acta con: 1) los temas tratados, 2) las decisiones tomadas y 3) los compromisos adquiridos. Se indicó que las actas de las reuniones solo quedan de forma digital, ya que no se formalizan con una firma física o digital, la única formalización es su envío a través del correo electrónico empresarial.

No manejan un estatuto orgánico, por lo que las funciones son las que van quedando establecidas para cada persona que labora en la empresa por la repartición verbal de funciones realizada inicialmente y por la costumbre de uso. Sin embargo, me indicaron que, en la reunión de directorio del 20 de marzo de 2018, se estableció el siguiente organigrama:

Gráfico 3

Organigrama operativo de Greenetics



Fuente: Greenetics Soluciones S.A.

Elaboración propia

1.3 Mercado y clientes

1. Concesionarias de vehículos como Cheviplan.

2. Colegios, como colegio Americano.

3. Empresas de servicios como Polygraph.

4. Movimientos políticos como Alianza País.

5. Empresas de servicios como Tecsago Tecnología y Servicios.

6. Municipios como DMQ.

No se registran contratos con empresas de los sectores financiero, banca privada o cooperativas de ahorro y crédito del sector popular y solidario.

1.4 Tamaño de la empresa

Número de empleados: Actualmente cuentan con un Gerente General, que a la vez es el Gerente Comercial, también cuentan con un Gerente de Técnico que también maneja la Gerencia Administrativa – Financiera, además cuentan con un ejecutivo de negocios y tres técnicos expertos en seguridad digital. Un total de seis personas en nómina. Por otro lado, se tiene profesionales que trabajan sin relación de dependencia, por actividad puntual, cinco técnicos para las capacitaciones y alrededor de 4 técnicos para los diversos contratos de servicios de seguridad prestados, tales como las consultorías y pruebas de penetración. También se maneja por contratos ocasionales la contabilidad de la empresa.

Impuesto a la renta:

Tabla 5

Gestión fiscal de Greenetics

Año fiscal	Impuesto a la Renta Causado
2017	$1,282.01
2016	$885.26
2015	$679.32
2014	$0.00

Fuente: (“SRI en Línea - Consulta de Impuesto a la Renta y Salida de Divisas” 2018)
Elaboración propia

1.5 Productos y servicios

La empresa Greenetics Soluciones S.A. se dedica exclusivamente a prestar servicios de seguridad digital, la propuesta de servicios es la siguiente:

1) Evaluación del Riesgo: Servicio mediante el cual se verifica qué y cuándo deben medirse los procesos y activos de seguridad digital, para identificar vulnerabilidades y amenazas. Permite desarrollar para el cliente la estrategia de seguridad de la información, considerando la exposición de sus activos al utilizar las tecnologías de la información, comunicación y la red de Internet. Normalmente por pedido de los clientes se basa en la ISO 27005 "Gestión de Riesgo en Seguridad de la Información".

2) Análisis de brechas de seguridad de la información: Servicio de consultoría mediante el cual se identifica el nivel de madurez del cliente frente a los estándares de seguridad de la información del sector al cual pertenece, por ejemplo, el sector bancario necesita cumplir las normas: ISO 27001, PCI DCS, JB-2014-3066.

3) Análisis de vulnerabilidades y test de penetración: En este tipo de servicio se busca descubrir las vulnerabilidades que un atacante podría explotar; se pone a prueba los sistemas informáticos, las aplicaciones del cliente, las políticas de seguridad de la información, el nivel de concienciación del personal y la exposición de los activos hacia el internet; todo esto manejado con los más altos estándares de confidencialidad y ética profesional. Se indagó en base a qué se puede asegurar el cumplir lo ofrecido en este servicio y se indicó que al momento es una afirmación netamente subjetiva.

4) Cursos de seguridad digital: Se pudieron identificar los siguientes cursos ofrecidos y entregados a los clientes desde sus aulas ubicadas en el edificio Smerald: Ethical Hacking básico, Ethical Hacking avanzado, Análisis Forense Informático, Ethical Hacking en Aplicaciones Web, Oficial de Seguridad de la Información y Gestión de Incidentes de Seguridad.

5) Gestión de seguridades (Outsourcing): Consiste en operar y administrar la infraestructura de seguridad instalada del cliente, así como del modelo de seguridad adoptado. Adicionalmente Greenetics incorpora sus plataformas y servicios a los existentes en el cliente, a fin de dar valor, con el menor impacto posible en la operación, con un monitoreo 7x24x365, y acuerdos de niveles de servicio (SLA) y reportes por incidentes, así como ejecutivos mensuales. Dentro de este servicio se puede incluir el monitoreo de un SOC o gestión de incidentes de un CSIRT, mediante

la alianza estratégica que al momento mantienen con CERT Cyberseg, la cual ya es parte de FIRST.

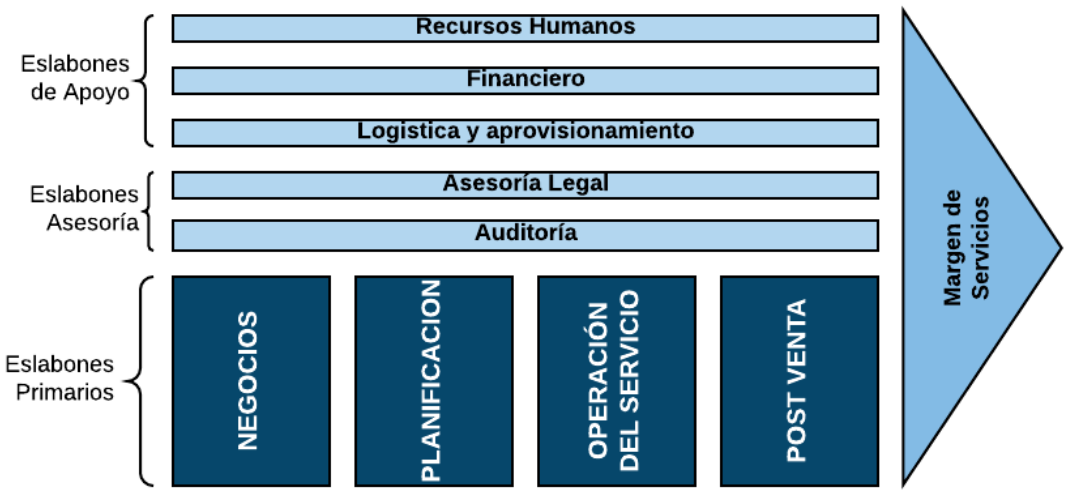
6) Análisis Forense Digital: El Análisis Forense Informático es un servicio entregado bajo demanda cuando una empresa ha sido víctima de un ataque, robo de información o pérdida de la misma, sobre el cual ofrecen las siguientes actividades: Análisis forense a digital (cualquier dispositivo electrónico), borrado seguro de información, recuperación de datos, análisis de Logs, acompañamiento como perito informático e informes periciales.

1.6 Cadena de valor

De las entrevistas a los ejecutivos de la empresa Greenetics, se pudo conocer que tienen un enfoque operacional en procesos, pero no cuentan formalmente con un documento que acredite que su operación está centrada en procesos. Sin embargo, de la información levantada se pudo establecer que el flujo de operación podría permitir identificar una cadena de valor como la que se muestra en el gráfico 4.

Gráfico 4

Cadena de valor de Greenetics



Fuente: Greenetics Soluciones S.A.

Elaboración propia

Las actividades correspondientes a los eslabones de apoyo son ejecutas por varios de los trabajadores de la empresa, pero principalmente por el Gerente Técnico.

Las actividades de los eslabones de Asesoría son contratadas externamente a la empresa únicamente cuando son necesarias en trabajos puntuales.

Las actividades de los eslabones primarios se ejecutan en una secuencia lógica de operación empresarial, manejándose con un dinamismo e informalidad propios de un emprendimiento de empresa de servicios MiPYME.

Negocios: Este es el punto inicial de la cadena de valor para la prestación de servicios, se encuentra totalmente enfocado al cliente, conlleva actividades como las propuestas comerciales, estructuración del equipo de ventas, publicidad y promociones. Es importante considerar la propiedad de intangibilidad de la prestación de los servicios, motivo por el cual es de suma importancia mostrar los servicios intangibles como productos tangibles.

Planificación: Este incluye el soporte físico y logístico necesario para la prestación del servicio, que permita al cliente lograr la experiencia del servicio, incluye las actividades de innovación, que permitan a la empresa mantener en el tiempo una prestación de servicios con una clara ventaja competitiva. Es aquí donde se diseñará los servicios a ser implementados, con un concepto de mejora continua, aplicando las mejores prácticas y lecciones aprendidas, todo sobre la base de la investigación y el desarrollo, que permitan estar a la vanguardia tecnológica, y del estado del arte en lo que tiene que ver a seguridad de la información.

Operación del servicio: En este proceso se interconectan todos los servicios prestados, realmente es el corazón de la empresa, incluye todas las actividades que se desarrollan al momento de prestar los servicios de la cartera de servicios propuesta.

Postventa: En este proceso se centra la interacción humana de la empresa para velar por la calidad del servicio prestado, buscando que sea la opinión del cliente tomado en cuenta para el rumbo que se le seguirá dando al negocio. La principal meta de este proceso es lograr la fidelización del cliente.

Margen de Servicios, Entrega de Valor: Es la consecuencia de todos los procesos agregadores de valor, como sumatoria de todas las ventajas competitivas logradas en los procesos internos de la empresa. Aquí se concentra la esencia del servicio prestado con todo su agregado de valor, es lo que le da a Greenetics una fortaleza que podría ser explotada para fidelizar al cliente. Los elementos que entregan valor se pueden sintetizar en: agilidad en respuesta por reducida burocracia interna, personal técnico certificado con un nivel elevado de conocimientos, reconocimiento

por las capacitaciones impartidas durante tres años, trabajos diseñados a la necesidad del cliente y una buena campaña de márquetin digital.

1.7 Experiencia específica de la Empresa

La principal experiencia de Greenetics reside en las capacitaciones impartidas durante tres años, en seguridad de la información, metodologías y herramientas de pruebas de penetración, análisis forense y formación de oficiales de seguridad; con más de 70 cursos y 1100 profesionales capacitados. Esto ha sido posible gracias a que la empresa cuenta con ingenieros certificados internacionalmente, como: ethical hackers Certified Ethical Hackers CEH e implementador líder en la norma ISO 27001.

En prestación de servicios de seguridad, Greenetics cuenta con una experiencia de cuatro años en el mercado de seguridad de la información, con más de 30 contratos finalizados a entera satisfacción de los clientes, con los debidos certificados de terminación conforme, entre los que se pueden destacar los siguientes:

- Ethical Hacking Interno y Externo a Cloudstudio.
- Ethical Hacking y Test de Penetración a Nimblersoftware.
- Test de Penetración Interno y Externo a Tecsago Tecnología y Servicios.
- Test de Penetración Interno y Externo a Movimiento Político Alianza PAIS.
- Ethical Hacking con Aseguramiento Tecnológico y outsourcing de seguridad a Polygraph.
- Ethical Hacking a la infraestructura de la Dirección Nacional de Comunicaciones de la Policía Nacional del Ecuador.
- Ethical Hacking a Chevyplan.
- Auditoría de Seguridad Informática a la infraestructura de ADHOC.
- Auditoría de Seguridad Informática a la Fundación Colegio Americano.

También se han tenido logros destacados a nivel internacional como empresa ganadora en la categoría de Eco-Reto en TIC Américas 2014 en la ciudad de Paraguay, participación en el Global TIC 2014 en Taiwán, participación en el International Multi-Conference on Society, Cybernetics and Informatics en Orlando, tercer puesto en The Youth Citizen Entrepreneurship Competition en Alemania, finalista en la liga de emprendedores extraordinarios de la CFN, ponencia en Latincacs 2017 ISACA en

Costa Rica, ponencia en el taller de auditoría de seguridad Informática 2018 de la Cámara de Bancos e Instituciones Financieras de Costa Rica y conferencia en el Security Congress Latin America 2018 en Chile.

2 Descripción del sector financiero.

El sector financiero de nuestro país está en constante crecimiento, según el sistema de provisión del Sector Financiero Popular y Solidario de la SEPS, en lo que respecta a los activos, que incluye los créditos otorgados, han pasado de 10,4 a 12,0 mil millones, lo que representa un incremento anual del 15,4 %; y en pasivos, que incluye los depósitos captados, han aumentado de 8,8 a 10,2 mil millones, esto es un incremento anual del 15,9%.

Tabla 6

Tasa de crecimiento del sector financiero 2016 - 2017

Cuenta	Sector	Dic-2016 (millones de USD)	Dic-2017 (millones de USD)	Tasa de crecimiento
Activos (incluye créditos)	Sector Financiero Popular y Solidario	10.397,5	11.994,3	15,4%
Activos (incluye créditos)	Banca Privada	35.599,1	37.936,3	6,6%
Pasivos (incluye depósitos)	Sector Financiero Popular y Solidario	8.827,5	10.235,2	15,9%
Pasivos (incluye depósitos)	Banca Privada	32.075,3	33.768,6	5,3%

Fuente: SEPS y SBP

Elaboración propia

2.1 Características generales

Dentro del sector financiero se han identificado tres segmentos de mercado a ser explotados, estos son: 1) segmento bancario, 2) sociedades financieras y 3) cooperativas de ahorro y crédito. Según la Superintendencia de Bancos (SB 2018), en

abril de 2018 operan en el Ecuador 23 instituciones bancarias privadas y 10 sociedades financieras, en tanto que de acuerdo con la Superintendencia de Economía Popular y Solidaria existen 64 cooperativas de ahorro y crédito de los segmentos 1 y 2 (SEPS 2017), mayor detalle de las 64 instituciones financieras consta en el anexo 1.

Las Cooperativas de Ahorro y Crédito actualmente se agrupan en seis asociaciones, las cuales son las que constan a continuación:

a) ICORED – Red de Integración Ecuatoriana de Cooperativas de Ahorro y Crédito
b) RFD – Red de Instituciones Financieras de Desarrollo
c) UCACSUR – Unión de Cooperativas de Ahorro y Crédito del SUR
d) UCACNOR - Unión de Cooperativas de Ahorro y Crédito del Norte
e) UCACCENTRO - Unión De Cooperativas De Ahorro Y Crédito Del Centro
f) FECOAC - Federación Nacional de Cooperativas de Ahorro y Crédito

Detalle de los datos utilizados para las entrevistas, tales como nombres de los dirigentes, dirección, teléfono, entre otros, constan en el anexo 2.

2.2 Sector Económico Popular y Solidario

Conforme manda el artículo 283 de la Constitución de la República del Ecuador, la economía popular y solidaria se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios (“Constitución” 2018, 166).

El artículo 1 de la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario, define a la economía popular y solidaria a la forma de organización económica, donde sus integrantes, individual o colectivamente, organizan y desarrollan procesos de producción, intercambio, comercialización, financiamiento y consumo de bienes y servicios, para satisfacer necesidades y generar ingresos, basadas en relaciones de solidaridad, cooperación y reciprocidad (“LOEPS” 2018, 3).

Las formas de organización de la economía popular y solidaria se definen según el artículo 8 en sectores comunitarios, asociativos y cooperativistas, así como las unidades económicas populares (“LOEPS” 2018, 5).

Las cooperativas de ahorro y crédito del segmento 1 corresponden a las instituciones que tienen activos superiores a USD 80 millones y las del segmento 2 son las que tienen activos entre USD 20 y USD 80 millones.

La seguridad de la información está regulada en el sector financiero y considera la responsabilidad en la administración del riesgo, que viene dado por las exigencias de seguridad conforme a las amenazas a las que están expuestas las entidades financieras y sus clientes, todo esto resguardado y supeditado a las políticas y procedimientos dictados por las entidades de regulación y control de este sector (SEPS 2013) (SB 2005).

2.3 Principales riesgos de seguridad informática del sector

Las necesidades del sector financiero giran en torno a la responsabilidad en la administración del riesgo, que viene dado por las exigencias de seguridad conforme a las amenazas a las que están expuestas las entidades financieras y sus clientes, todo esto resguardado y supeditado a las políticas y procedimientos dictados por las entidades de regulación y control de este sector.

Principalmente podemos mencionar la exigencia que según la vigente Resolución JB-2014-3066 y 128-2015-F, tienen las instituciones financieras de implementar medidas de seguridad en los diferentes canales electrónicos, a través de los cuales brindan servicios a sus clientes, así como de mejorar los controles de gestión de la tecnología de la información y comunicaciones, de mejorar la gestión del riesgo operativo y de implementar medidas de seguridad que mitiguen los fraudes relacionados con los cajeros automáticos.

Es necesario mencionar el incremento de ataques informáticos, así como de vulnerabilidades que involucran a los activos de información del sistema financiero, lo que significa para el sector financiero de cooperativas de ahorro y crédito un aumento significativo del riesgo de la seguridad de la información, que ha exigido a la Superintendencia de Economía Popular y Solidaria, SEPS, a emitir regulación complementaria, tales como:

1. Control de seguridades en el uso de transferencias electrónicas SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 y su reforma SEPS-IGT-IR-ISF-ITIC-IGJ-2017-113.
2. Norma de Control para la seguridad física y electrónica SEPS-IGT-IR-IGJ-2018-021.
3. Norma de control para el envío y recepción información y notificaciones SEPS-IGT-IR-IGJ-2018-016.

2.4 Cumplimiento de la normativa de seguridad

El artículo 444 del Código Orgánico Monetario y Financiero, determina que las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación Monetaria y Financiera y al control de la Superintendencia de Economía Popular y Solidaria, quienes en las políticas que emitan tendrán presente la naturaleza y características propias del sector financiero popular y solidario.

El artículo 163 del referido Código, determina que las cooperativas de ahorro y crédito, las cajas centrales y las asociaciones mutualistas de ahorro y crédito para la vivienda forman parte del sector financiero popular y solidario

El punto 2.4 de la Resolución JB-2014-3066 que en cuarto numeral indica: "2.44 Incidente de seguridad de la información.- Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información;" define lo que es un incidente de seguridad de la información, actividad que en caso de ser manejada por una empresa externa de prestación de servicios, debe considerar los más altos estándares de seguridad de la información, para mantener el nivel de confianza del cliente financiero y evitar poner en riesgo la credibilidad y trayectoria de la institución financiera.

2.5 Estadísticas e indicadores de los organismos de regulación

En los últimos años la economía popular y solidaria ha cobrado importancia y se ha extendido dentro del sector financiero del Ecuador, lo que se puede apreciar en la tabla 7, con el persistente crecimiento desde el año 2013 y donde se muestra el crecimiento semestral comparativo respecto de la banca privada.

Tabla 7

Comparativo entre banca privada y economía popular y solidaria

	Sector Financiero Banca Privada	Sector Financiero Economía Popular y Solidaria	Comparativo
Jun 2013	0,6%	7%	↑ 6,4 %
Dic 2013	9,6%	9,5%	↓ 0,1 %
Jun 2014	1,9%	6,9%	↑ 5,0 %
Dic 2014	7,3%	7,4%	↑ 0,1 %
Jun 2015	-4,4%	3,7%	↑ 8,1 %
Dic 2015	-4%	0,6%	↑ 4,6 %
Jun 2016	4,9%	4,9%	-
Dic 2016	9,9%	10,3%	↑ 0,4 %
Jun 2017	4,5%	9,4%	↑ 4,9 %
Dic 2017	4,7%	7,8%	↑ 3,1 %

Fuente: SEPS y SBP

Elaboración propia

Al momento existen cooperativas de ahorro y crédito que son más grandes que algunos de los bancos medianos y pequeños, tal es el caso de: 1) la Juventud Ecuatoriana Progresista, 2) el Jardín Azuayo y 3) la Policía Nacional, cuyas carteras brutas sumadas dan más de 2,16 mil millones de dólares, lo que es mayor a la cartera de tres de los bancos medianos y los 11 bancos pequeños del país, que sumados los catorce bancos dan un total de 1,79 mil millones en su orden respectivo: 1)Citibank, 2)Loja y 3)Machala; 1)Procredit, 2)Amazonas, 3)Comercial Manabí, 4)Litoral, 5)Coopnacional, 6)Capital, 7)Finca, 8)Del Bank, 9)D-Miro, 10)Bancodesarrollo, 11)Visionfund.

En lo que tiene que ver con el control realizado por la Superintendencia de Economía Popular y Solidaria SEPS, cada año se han incrementado el número de supervisiones en campo a nivel nacional hacia las Cooperativas de Ahorro y Crédito, según se puede apreciar en el siguiente cuadro que consta esquematizado en la tabla 8.

Tabla 8

Inspecciones realizadas por la SEPS

	2012	2013	2014	2015	2016	2017
Entidades supervisadas *insitu*	5	66	223	381	479	541
Visitas realizadas	5	77	280	584	802	954

Fuente: SEPS

Elaboración propia

Capítulo tercero
Metodología

1 Diseño y alcance de la entrevista y la encuesta

Para la investigación de mercado se ha considerado utilizar fuentes primarias de datos, esto a través de entrevistas y encuestas, a fin de poder generar información del mercado financiero cooperativo, así como identificar sus problemas y necesidades.

Una investigación de mercado, con resultados claros, contribuirá con los insumos necesarios para planear la estrategia de Greenetics Soluciones, en función de algunos de los objetivos del mercado financiero popular y solidario, así como de algunos de los objetivos de las cooperativas de ahorro y crédito. La investigación de mercado estará en torno a las necesidades de los clientes, para la solución de sus problemas de seguridad de la información, que nos permitan agregar valor en las propuestas, específicamente hacia los clientes del sector financiero de cooperativas.

El análisis e interpretación de los resultados obtenidos de los dos instrumentos identificados para realizar el estudio de mercado, esto es las entrevistas y las encuestas, permitirán tener mayor claridad de las actividades a desarrollarse para la reorientación estratégica de la empresa Greenetics Soluciones. Esto facilitará la generación de una planificación cimentada en una estrategia que considerará factores importantes para el sector financiero como son: la calidad y la seguridad de la información, ya que las instituciones las tienen plasmadas entre algunas de sus necesidades y oportunidades.

La realización de las entrevistas y encuestas se ha dimensionado y planificado de acuerdo con las facilidades logradas de manera verbal con el Comité de Seguridad Bancaria del Ecuador, con la Red de Integración Ecuatorianas de Cooperativas de Ahorro y Crédito, con la Federación Nacional de Cooperativas de Ahorro y Crédito y a la utilización de los datos estadísticos obtenidos de la Superintendencia de Bancos y de la Superintendencia de Economía Popular y Solidaria.

1.1 Obtención de la muestra para la encuesta y la entrevista

Para definir los fundamentos del muestreo, es importante identificar la población, sobre la base del total de los elementos que la conforma. En este caso se

ha identificado como población universo a todas las cooperativas de nivel 1, que suman 26 instituciones, con un total de activos de $ 8.151.837.413,32 USD; y a las cooperativas de nivel 2, que suman 38 instituciones, con un total de activos de $ 1.815.073.913,01 USD. Lo que nos da una población de 64 cooperativas con un total de $ 9.966.911.326,33 USD en activos.

Se realizó el levantamiento de encuestas a ocho cooperativas de ahorro y crédito bajo un enfoque empírico cuantitativo, esto se puede apreciar en la tabla 9.

Tabla 9

Activos de las Cooperativas en millones de dólares

Nombre Cooperativa	Activos (Millones USD)	Porcentaje
Juventud Ecuatoriana Progresista Ltda	1.619	19,86 %
Jardín Azuayo Ltda	773	9,49%
Policía Nacional Ltda	711	8,72%
Cooprogreso Ltda	452	5,55%
29 De Octubre Ltda	438	5,38%
Oscus Ltda	338	4,15%
San Francisco Ltda	311	3,82%
Riobamba Ltda	286	3,51%
Total 8 Cooperativas más significativas	4.931	60,49%

Fuente: (“SEPS” 2018)

Elaboración propia

El total de activos de los segmentos 1 y 2 de las cooperativas suman $ 9.966.911.326,33 USD, por lo que con las 8 cooperativas consideradas para la encuesta se ha cubierto un 60,49% del total de activos de estos dos segmentos de las cooperativas de ahorro y crédito.

Tabla 10

Ficha descriptiva del muestreo:

1. Universo:	Cooperativas de Ahorro y Crédito de nivel 1 y 2
2. Unidades de Muestreo:	Cooperativas que, de acuerdo con sus activos, suman al menos el 50 % del total de activos, respecto del Universo
3. Alcance:	Nacional
4. Tiempo:	2018

Fuente: (“SEPS” 2018)

Elaboración propia

Se realizaron 5 entrevistas, utilizando un enfoque empírico cualitativo, dos de las cuales fueron efectuadas a los gerentes de cooperativas de ahorro y crédito conocedores de la seguridad de la información en el sector financiero, una para el segmento 1 y la otra para segmento 2, para poder tener una primera perspectiva sectorial individual; adicionalmente se realizaron tres entrevistas a los directivos de las asociaciones de cooperativas, con la finalidad de tener una segunda perspectiva gremial.

1.2 Diseño de la entrevista

Están dirigidas a los gerentes institucionales de las cooperativas de ahorro y crédito, así como a los directivos de las asociaciones del sector financiero popular y solidario.

Para el diseño de la entrevista se considera un razonamiento deductivo ya que se parte de lo general hacia lo particular, como punto de inicio se inicia entrevistando al directivo de la cooperativa con la pregunta más general, esto es indagando ¿si el riesgo es un factor importante, a ser tomado en cuenta en la planificación y operación de una cooperativa de ahorro y crédito?, para luego hacer la pregunta un poco más específica, que es conocer ¿si está de acuerdo en apartar un presupuesto a fin de que sea utilizado en acciones específicas para mitigar el riesgo?

De acuerdo con el método deductivo se plantea una tercera pregunta: ¿Si la regulación es un factor que obliga a destinar un presupuesto hacia temas que no son el centro de la operación financiera, como la calidad y la seguridad de la información? Con esto se pretende conocer si está al tanto de las más recientes regulaciones del sector financiero, en materia de seguridad y calidad, y si las inversiones previstas han sido consideradas en función del cumplimiento regulatorio; esto nos permitirá conocer que tan influyente es la regulación en este sector, considerando que este factor externo es uno de los más influyentes en la matriz de evaluación de factores externos.

Una vez que se ha entrado en materia presupuestaria, se ha considerado preguntar: ¿Si considera este tipo de presupuesto como un gasto o una inversión? Con la intención de conocer el grado de madurez de la institución, ya que aún persiste el concepto de considerar la calidad y la seguridad como un gasto, producto de la exigencia normativa y no como una oportunidad de agregar valor al cliente con un

consecuente retorno a la inversión, para el caso de la seguridad conocido como ROSI, Return Of Security Investment.

Con la pregunta ¿Si considera adecuado contar con un departamento permanente de gestión de riesgo? Estamos en la capacidad de conocer, no solo si están invirtiendo en seguridad, sino también, estar al tanto si considera ésta una actividad permanente de la institución, que cuenta con profesionales especializados, con la capacidad de conducir con directrices técnicas a la cooperativa en la contención, mitigación y transferencia del riesgo.

¿Si la confianza es un pilar fundamental para la operación de una entidad del sector financiero popular y solidario? Es una pregunta que permite ir entrando aún más en contexto de qué tan profundo dentro de la cultura institucional se encuentra el tema de la confianza, que emana de la seguridad y la calidad; es importante conocer para poder si esta cultura sería exigible a sus proveedores de servicios, especialmente en materia de seguridad, donde la confianza es un factor clave.

Ahora se procura conocer si estas mismas consideraciones de confianza se perciben como necesarias desde los proveedores, como una cadena de confianza que también debe nacer desde las empresas que prestan servicios de tipo sensible a la cooperativa.

También se desea conocer qué tan importante puede resultar la capacitación en temas satélites de la operación principal de la cooperativa, tales como la seguridad de la información y la calidad, así como la perpetuidad en este tipo de formación.

Para finalizar se realiza al entrevistado dos preguntas claves para la reorientación estratégica ¿si los proveedores de servicios que manejan información sensible y características de prestación delicadas frente a la confianza de sus clientes deben contar con certificaciones formales para la gestión de la seguridad de la información y la prestación de servicios con niveles óptimos de calidad?

1.3 Diseño de la encuesta

La encuesta está dirigida a los profesionales técnicos, conocedores de la temática de seguridad de la información, pertenecientes al área de tecnologías de la información o al área de gestión de riesgos.

Para la encuesta se ha considerado un sector representativo de las Cooperativas de Ahorro y Crédito, esto es las 8 cooperativas más significativas en términos de

activos de capital, que actualmente tienen un 60,49%, del total de activos, estas son: Juventud Ecuatoriana Progresista Ltda, Jardín Azuayo Ltda, Policía Nacional Ltda, Cooprogreso Ltda, 29 De Octubre Ltda, Oscus Ltda, San Francisco Ltda y Riobamba Ltda.

Para el diseño de la encuesta se manejaron dos ejes principales, para el eje vertical se consideró ir desde lo general hacia lo particular, mientras que para el eje horizontal se aplicó cuatro aspectos que son: los riesgos, la seguridad de la información, la calidad en la prestación de los servicios y los paralelismos de confianza hacia los proveedores.

Se elaboraron 24 preguntas, divididas de la siguiente manera: 6 para riesgos, 9 para seguridad de la información, 6 para gestión de la calidad y 3 para el paralelismo de confianza.

2 Presentación de resultados de las entrevistas y de las encuestas

Las entrevistas y las encuestas fueron realizadas de forma simultánea, entre el 18 de junio de 2018 y el 19 de agosto de 2018, aprovechando algunas reuniones con las asociaciones de cooperativas o en sesiones particulares. Finalmente se pudieron realizar las 8 encuestas planificadas y 5 adicionales, con un total de 13 encuestas que se encuentran en el anexo 3; y se logró entrevistar a 5 dirigentes del sector financiero popular y solidario, que se adjuntan en el anexo 4.

2.1 Tabulación cualitativa de resultados de la entrevista

De la pregunta uno, se pudo establecer qué el riesgo es un factor importante para tomar en cuenta en la planificación y operación de una Cooperativa de Ahorro y Crédito, por cuanto está considerado en la regulación dada por la SEPS, que es un factor de mucha importancia para todos los entrevistados, como por que si agrega valor a la situación de la institución financiera.

Respecto a la segunda pregunta se puede concluir que les es muy importante mitigar el riesgo, consideran en efecto que es necesario destinar presupuesto en seguridad de la información o en la calidad de los procesos de atención a los clientes, se indicó que el factor tecnológico es uno de los principales factores de riesgo y más aun si se lo asocia al tema de seguridad de la información y la realidad de que todo va

al internet, en el caso de las cooperativas toma mucha relevancia las transacciones digitales en línea.

Respecto de la pregunta número tres, los entrevistados estuvieron de acuerdo por unanimidad que la regulación es uno de los principales motivos para destinar presupuesto en temas externos al núcleo de la operación financiera, ya que normalmente se entiende como inversión a todo lo que está alineado a la operatividad de la institución financiera, que no es el caso de la seguridad de la información y la calidad en la prestación de los servicios, rubros que normalmente se los considera un gasto, necesarios para cumplir con la regulación.

Desde la perspectiva gremial se considera que la seguridad de la información es un gasto que normalmente se considera en el presupuesto por motivos más bien regulatorios, en la perspectiva institucional de las tres posturas, dos estuvieron de acuerdo que se puede considerar como una inversión, frente a lo cual esperan un retorno a su inversión.

Para los presupuestos destinados a mejorar la postura de calidad en los servicios prestados a los clientes, es interesante observar que la postura gremial cambia respecto del punto anterior ya que sí están más familiarizados con la calidad y de cómo ésta pude ser un factor que en el mediano y largo plazo puede retribuir su inversión. Por el otro lado la posición institucional es muy similar, con una claridad de que una inversión en calidad no solo les permitirá mantener a los actuales clientes, sino que también les permitirá aumentar su cartera de clientes.

Aun no le ven la ventaja de destinar importantes recursos a tener un departamento de gestión de riesgos permanentemente, aún persiste algún grado de confusión con las actividades que desempeña la gerencia de tecnologías de la información; la posición es aún más radical para los directivos de las asociaciones que ven esta medida para las cooperativas pequeñas de los sectores N4 y N5 como un paso innecesario, para la posición institucional hay un cierto margen de escepticismo, sin embargo no están en desacuerdo en que exista de forma permanente una gerencia de gestión de riesgos.

Los cinco entrevistados estuvieron de acuerdo en mayor o menor medida, con el concepto de que es un pilar fundamental para mantener una aceptación de sus clientes, el factor de la confianza, por eso indican que muchas instituciones financieras toman el valor de la confianza como parte de su eslogan comercial, incluso han desarrollado productos que se cimientan sobre este valor.

Así como sus clientes les exigen un gran número de buenas conductas para ser merecedores a su confianza, considera que la confianza es también un factor fundamental y endosable a sus proveedores, en especial a los que manejan datos sensibles de sus instituciones, para lo cual deben también cumplir estándares de seguridad de la información y calidad, que garanticen la operatividad en la prestación de los servicios.

La capacitación en temas como seguridad de la información y calidad en la prestación de servicios son considerados como necesarios, para que sean impartidos a los empleados de la cooperativa; sin embargo, no ven la necesidad del todo de que esta formación profesional deba de tener un carácter de permanente y mucho menos de que deban pagar altas sumas de dinero para capacitar y certificar internacionalmente a sus profesionales.

Es muy importante para los directivos y para los gerentes de las instituciones del sector financiero popular y solidario, que sus proveedores de servicios sensibles cuenten con certificaciones de buen manejo de la información, ya que existe la preocupación de qué pasaría si esta información sensible saliera de la institución y cayera en malas manos; por un lado indican que esta información puede ser utilizada para causar un daño a la imagen de la institución financiera, por otro lado se piensa que pueden utilizar la información técnica para atacar a la cooperativa de ahorro y crédito.

Es muy deseable que los proveedores de servicios sensibles cuenten con una certificación de calidad en la prestación de sus servicios, sin embargo, no consideran que sea una medida del todo contundente para dejar fuera un proveedor que no cuenta con este nivel de certificación.

2.2 Tabulación cuantitativa de resultados de la encuesta

Pregunta 1. ¿Su conocimiento sobre riesgos es? En esta pregunta muy general se busca un primer acercamiento, que se esperaría sea positivo y de un nivel alto, para lo cual se segmentó la posible respuesta en cinco alternativas: Conocimiento bajo, significa que no tiene ninguna formación ni conocimiento de la materia, por lo que se trata de una persona que no está bien ubicada o el nivel de madurez institucional es tan bajo, que no se ha previsto una persona experta para esta área de la institución; conocimiento medio, es una persona que está en una fase de aprendizaje, muchas veces

porque siempre ha estado en el área y se empieza a formar en la temática del riesgo, debido a un giro institucional en esta materia muchas veces por tema regulatorio; conocimiento alto, es la respuesta esperada ya que corresponde a profesionales que conocen la normativa sectorial de la SEPS y pueden aplicarla de manera adecuada; conocimiento muy alto, es cuando ya existe un interés adicional que ha permitido al profesional del área investigar, participar en foros nacionales e internacionales, leer literatura al respecto; conocimiento completo, se refiere a la persona que incluso tiene una formación altamente especializada, con certificaciones internacionales, tales como una ISO 31000 o una ISO 27005 ("cigras2011-cserra-presentacion1 modo de compatibilidad.pdf" 2018).

Tabla Nº11:

Tiene conocimientos sobre riesgos

Opción	Resultado
Completo	15,4%
Muy alto	15,4%
Alto	46,1%
Medio	15,4%
Bajo	7,7%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 2. ¿Tiene alguna capacitación en riesgos? Con esta pregunta se procura validar cómo la capacitación puede influir en el conocimiento del riesgo, por lo que fue planteada una pregunta cerrada a ser contestada con: Sí o No, con la intención de conocer la brecha de conocimiento de capacitación en riesgos.

Tabla Nº 12:

Tiene capacitaciones sobre riesgos

Opción	Resultado
Sí	46,1%
No	53,9%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 3. ¿Existe la cultura de riesgo en su cooperativa? Se quiere conocer si existe una implantación de gestión del riesgo de forma transversal al accionar institucional, o si mejor aún conoce fehacientemente que existe un marco de operación que incorpora de forma oficial los temas de riesgo, esto es un plan ordenado que obliga como normativa interna la gestión del riesgo. Por este motivo, pese a ser una pregunta cerrada a obtener una respuesta de Sí o No, se dejó la posibilidad de poder responder de manera incierta en caso de no conocer sobre la pregunta realizada.

Tabla Nº 13:

Existe cultura del riesgo

Opción	Resultado
Sí	69,3%
No	23,0%
No sabe	7,7%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 4. ¿Su conocimiento sobre riesgo operativo es? Se plantea aterrizar el concepto de riesgo, a algo más práctico y cercano a la seguridad de la información y a la gestión de la calidad, como lo es el riesgo operativo, por lo que la pregunta agudiza más los cuestionamientos iniciales, al enfocarse directamente en el riesgo operativo. Par poder identificar de mejor manera las respuestas de los encuestados, se realizó una graduación de cinco pasos, donde un conocimiento bajo significa que el profesional estaría administrativamente mal ubicado y debería ser trasladado a otra área de la institución; un conocimiento medio indicaría que es una persona en formación, ya sea porque recién entró a la institución o es nuevo en el área, porque recién ha iniciado su formación en riesgo operativo, o que tiene una formación en riesgo de nivel alto que le permite considerar tener un conocimiento medio en riesgo operativo; un conocimiento alto en riesgo operativo indica que está en la capacidad de manejar cualquier tema de la institución respecto de su accionar frente a la regulación sectorial; un conocimiento muy alto indica que tiene una formación académica en riesgo

operativo y experiencia superior a los 3 años; finalmente un conocimiento completo denota un dominio de la materia, esto es tener certificaciones internacionales y participación en equipos de gestión de riesgo operativo y más de 7 años de experiencia en riesgo operativo.

Tabla Nº 14:

Conocimiento sobre riesgo operativo

Opción	Resultado
Completo	23,0%
Muy alto	23,0%
Alto	38,5%
Medio	15,5%
Bajo	0
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 5. ¿Se gestiona el riesgo operativo en su cooperativa? Es muy necesario conocer si existe dentro del plan estratégico de la cooperativa la gestión del riesgo operativo con planes de acción objetivos que permitan contener, mitigar, remediar, asumir o transferir el nivel de riesgo operativo; esto nos permitirá conocer las acciones de seguridad de la información y calidad para lograr estos objetivos institucionales. Para este efecto se ha considerado una pregunta cerrada a Sí y No, con la opción de no saber si formalmente existe una gestión de riesgo dentro de la institución.

Tabla Nº 15:

Gestión del riesgo operativo

Opción	Resultado
Sí	84,6%
No	7,7%
No sabe	7,7%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 6. ¿Qué factores influyen sobre el riesgo operativo? Agudizando más la pregunta, se necesita conocer las causas más comunes para la existencia del riesgo operativo, motivo por el cual de las entrevistas se toma las opciones consideradas como origen, por lo cual se dieron cinco opciones de respuesta ligadas a la operación de la institución.

Tabla Nº 16:

Factores que influencian el riesgo operativo

Opción	Resultado
Procedimientos	15,4%
Empleados	16,4%
Tecnología	25,6%
Clientes	19,5%
Ataques informáticos	23,1%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 7. ¿Tiene conocimiento sobre los riesgos en seguridad de la información, y las consecuencias que puede ocasionar un ataque informático? Se requiere conocer puntualmente el nivel de conciencia respecto de la seguridad de la información en los niveles de riesgo operativo, o si se maneja el concepto de riesgo de seguridad de la información, para lo cual se planteó esta pregunta cerrada con únicamente la opción de Sí o No.

Tabla Nº 17:

Existen riesgos en seguridad de la información

Opción	Resultado
Sí	61,5%
No	38,5%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 8. ¿Los ataques informáticos pueden provocar riesgo operativo? Esta pregunta en el fondo lo que pretende conocer es si el profesional ya ha tenido una experiencia de ataque, y si pudo relacionar este ataque con el riesgo operativo.

Tabla Nº 18:

Los ataques informáticos provocan riesgo operativo

Opción	Resultado
Sí	69,2%
No	15,4%
No sabe	15,4%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 9. ¿En su cooperativa disponen de un plan de seguridad de la información? Se busca conocer si como medida preventiva en función del riesgo operativo y de posibles ataques sufridos, han tomado la iniciativa de tener un plan de seguridad de la información. Se ha propuesto una respuesta cerrada de Sí o No, con la alternativa de desconocimiento, para asegurar que el si, sea en firme y poder conocer en efecto cuantas cooperativas de las entrevistadas cuentan con un plan de seguridad de la información.

Tabla Nº 19:

Existe un Plan de Seguridad de la Información

Opción	Resultado
Sí	46,1%
No	38,5%
No sabe	15,4%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 10. ¿Tiene alguna capacitación en seguridad de la información? Se busca complementar la pregunta anterior, con el tema de capacitación. El que los profesionales que conocen del plan de seguridad tengan capacitación, favorecerá al éxito de la implantación y operación del citado plan. Es una pregunta cerrada a Sí o No, para en realidad saber si las personas que conocen de seguridad tienen una formación empírica o por el contrario su conocimiento de la materia es formal.

Tabla Nº 20:

Capacitación en seguridad de la información

Opción	Resultado
Sí	46,2%
No	53,8%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 11. ¿Su Plan de seguridad de la información se alinea al objetivo del negocio? Es necesario conocer la cercanía que tiene el plan de seguridad de la información a los objetivos institucionales, ya que esto posibilita una mejor respuesta de la alta gerencia, así como del resto de la organización; un plan alineado a los objetivos empresariales permite desplegar como inversión muchas soluciones y trazar planes de acción que por lo general deben ser respaldados por una empresa externa. Es una pregunta cerrada de repuesta Sí o No, ya que no cabe parcialidades, si el plan está bien trazado, necesariamente estará alineado a los objetivos empresariales, caso contrario será solo un documento más, que posiblemente fue desarrollado a la ligera, sin ninguna expectativa.

Tabla Nº 21:

El plan de seguridad de la información está alineado a los objetivos

Opción	Resultado
Sí	38,5%
No	61,5%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 12. ¿Se difunde adecuadamente el plan de seguridad de la información? La difusión del plan de seguridad de la información es parte integral del plan, pero no siempre sucede esto, por lo que es importante conocer si en efecto existe una difusión, que permita aplicar las políticas de seguridad por parte de todos los involucrados, esto es directivos, especialista en seguridad, personal general, proveedores, clientes. Es una pregunta cerrada con opción de Sí o No, ya que se espera que haya difusión asociada al plan o de plano que no la haya.

Tabla Nº 22:

Difusión del Plan de seguridad de la información

Opción	Resultado
Sí	23,0%
No	77,0%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 13. ¿Se evalúa el plan de seguridad de la información? Para que el plan de seguridad de la información tenga éxito, debe ser evaluado, en caso de no serlo, los objetivos planteados en este son subjetivos y pueden cumplirse o no a criterio de la persona designada como responsable del cumplimiento del plan; un plan que no es evaluado no permite hacer control y no permite mejorarlo, por lo que se ha considerado como una pregunta cerrada, con opción de Sí o No, y una alternativa de desconocimiento en caso de que la persona no esté en contacto con este proceso.

Tabla Nº 23:

Evaluación del plan de seguridad de la información

Opción	Resultado
Sí	15,4%
No	46,1%
No sabe	38,5%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 14. ¿Los controles de sus planes seguridad de la información contribuyen a minimizar los problemas operativos? Los controles implementados pueden ser diversos, no necesariamente bien seleccionados para minimizar los riesgos operativos, motivo por el cual se hace interesante poder conocer la percepción de satisfacción en torno de los controles desplegados para el plan de seguridad de la información. Como conocemos ISO 27001 por ejemplo con controles en su anexo A, que se refuerzan con los controles de la ISO 27002 e ISO 27015. Esta pregunta cerrada a respuesta de Sí, No o desconocimiento.

Tabla Nº 24:

Los controles del plan de seguridad de la información

Opción	Resultado
Sí	23,0%
No	38,5%
No sabe	38,5%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 15. ¿Los incidentes ocurridos por un alto riesgo operativo pueden producir pérdidas económicas? Se desea conocer la ocurrencia de incidentes de seguridad y si estos han afectado la operatividad, con la consecuente pérdida de funcionalidad que haya producido pérdidas económicas a la institución financiera popular y solidaria, por un lado, conocer el grado de significancia de los incidentes de seguridad de la información sobre las pérdidas económicas. Esta pregunta cerrada a respuesta de Sí, No o desconocimiento.

Tabla Nº 25:

Pérdidas económicas por riesgo operativo

Opción	Resultado
Sí	61,5%
No	23,1%
No sabe	15,4%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 16. ¿Su conocimiento sobre mejoramiento continuo y gestión de la calidad es? Se necesita conocer el grado de conocimiento sobre mejoramiento continuo y gestión de la calidad, que puede parecer muy trivial, sin embargo, en muchas instituciones no se tiene personal capacitado en esta temática. Se han dado cinco opciones de respuesta, conocimiento básico cuando no tiene ninguna noción de la gestión de la calidad, medio cuando tiene conocimientos básicos o está iniciando un proceso de aprendizaje, nivel alto cuando su conocimiento le permite gestionar la conformidad y permanencia de los clientes, así como el cumplimiento regulatorio en temas de calidad, nivel muy alto cuando tiene una vasta formación y una experiencia de al menos tres años en temas de calidad y mejoramiento continuo, conocimiento completo cuando se trata de un profesional certificado en temas de calidad, con experiencia en auditorias de calidad, con un tiempo no menor a los 5 años.

Tabla Nº 26:

Conocimiento sobre gestión de la calidad

Opción	Resultado
Completo	15,4%
Muy alto	15,4%
Alto	38,5%
Medio	23,0%
Bajo	7,7%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 17. ¿Se tiene un Plan de Mejora Continua o Gestión de la Calidad en su cooperativa? Se necesita conocer si en la institución financiera han considerado formalmente un plan de gestión de la calidad, lo cual tiene una incidencia directa en el riesgo operativo por la satisfacción del cliente. La respuesta es cerrada a Sí, No y no sabe.

Tabla Nº 27:

Existencia de un Plan de Gestión de la Calidad

Opción	Resultado
Sí	53,8%
No	30,8%
No sabe	15,4%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 18. ¿Tiene alguna capacitación en mejora continua o gestión de la calidad? Se busca complementar la pregunta anterior con el tema de capacitación, el que los profesionales que conocen del plan de gestión de calidad tengan capacitación, favorecerá al éxito de la implantación y operación del plan. Es una pregunta cerrada a Sí o No, para en realidad saber si las personas que conocen de calidad total tienen una formación empírica o por el contrario su conocimiento de la materia es formal.

Tabla Nº 28:

Capacitación en Gestión de la calidad

Opción	Resultado
Sí	77%
No	23%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 19. ¿Su Plan de Gestión de la Calidad se alinea al objetivo del negocio? Es necesario conocer la cercanía que tiene el plan de gestión de la calidad a los objetivos institucionales, ya que esto posibilita una mejor respuesta de la alta gerencia, así como del resto de la organización; un plan alineado a los objetivos empresariales permite desplegar como inversión muchas soluciones y trazar planes de acción que por lo general deben ser respaldados por una empresa externa. Es una pregunta cerrada de repuesta Sí o No, ya que no cabe parcialidades, si el plan está bien trazado, necesariamente estará alineado a los objetivos empresariales, caso contrario

será solo un documento más, que posiblemente fue desarrollado a la ligera, sin ninguna expectativa real de cumplimiento.

Tabla Nº 29:

Plan de Gestión de la Calidad alineado a los objetivos institucionales

Opción	Resultado
Sí	38,5%
No	23,0%
No sabe	38,5%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 20. ¿Los controles de sus planes de calidad contribuyen a minimizar los problemas operativos? Los controles implementados pueden ser diversos, no necesariamente bien seleccionados para minimizar los riesgos operativos, motivo por el cual se hace interesante poder conocer la percepción de satisfacción en torno de los controles desplegados para el plan de gestión de calidad, como conocemos ISO 9001 incluye varios controles en este sentido. Esta pregunta cerrada.

Tabla Nº 30:

Controles al Plan de Gestión de la Calidad

Opción	Resultado
Sí	38,5%
No	15,4%
No sabe	46,1%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 21. ¿Qué nivel de fidelidad de los clientes se puede lograr, al mantener un plan de calidad que tome en cuenta sus requerimientos considerando: cumplimiento, tiempos de atención y adecuado trato? Se pretende conocer qué grado de madurez se tiene respecto de la gestión de calidad, si el concepto de fidelidad del cliente se lo tiene ligado al tema de la calidad de la prestación de los servicios. Nivel

bajo si se piensa que no tiene nada que ver la fidelidad con la calidad, nivel medio si puede tener algún efecto menor, nivel alto cuando sí hay una relación directa, nivel muy alto cuando hay una madurez institucional en la gestión de la calidad y cualquier variación en la calidad reflejara una mayor o menor permanencia del cliente, completo cuando toda acción en lo referente a la calidad puede significar una decisión del cliente.

Tabla Nº 31:

Nivel de fidelidad de clientes al tener gestión de calidad

Opción	Resultado
Completo	30,8%
Muy alto	38,4%
Alto	23,1%
Medio	7,7%
Bajo	0
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 22. ¿Es necesario firmar con sus proveedores un NDA? Es necesario conocer si mantienen políticas de confidencialidad mínimas como lo es la suscripción de un NDA con sus proveedores. Es una pregunta cerrada a Sí y No.

Tabla Nº 32:

Firma de NDA

Opción	Resultado
Sí	92,3%
No	7,7%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 23. ¿Es importante que sus proveedores tengan un código de ética? Dentro de la reorientación estratégica está el desarrollar un código de ética para Greenetics, por lo que resulta necesario conocer si este documento genera valor para

los profesionales encuestados de las instituciones financieras. La pregunta es cerrada a una respuesta de Sí o No.

Tabla Nº 33:

Importancia del Código de ética

Opción	Resultado
Sí	84,6%
No	15,4%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Pregunta 24. ¿Considera que sus planes de seguridad de la información o calidad deben favorecer a proveedores que cuentan con planes similares? Es necesario conocer el nivel de compromiso esperado hacia los proveedores en materia de seguridad de la información y si es de valor que éstos cuenten con planes de seguridad similares para poder mantener una relación comercial. La pregunta es cerrada a Sí o No como respuesta.

Tabla Nº 34:

Planes de seguridad o calidad en proveedores

Opción	Resultado
Sí	77,9%
No	22,1%
Total	100%

Fuente: Encuesta: Investigación de Campo

Elaboración propia

Capítulo cuarto
Análisis de resultados

1 Análisis de resultados de la entrevista

El riesgo es el punto de partida para proteger los activos, actividades y recursos relacionados a sus instituciones, esta aseveración se cimienta en la regulación vigente y las mejores prácticas del sector financiero. Ninguno de los entrevistados tiene alguna objeción en proceder bajo esta metodología de trabajo, por el contrario, indican que el tema del riesgo se maneja desde los niveles gerenciales más representativos de sus respectivas organizaciones. El riesgo siempre llama a la acción, desde la reestructuración interna de sus instituciones, creando unidades especializadas, comités administrativos, consejos de vigilancia para la administración del riesgo, hasta el establecimiento de planes de acción en base a una matriz de riesgos, que les permita mitigarlos y reducir su impacto.

Sin embargo, de la consideración de trabajar en función de reducir los factores que ponen en riesgo su institución, indicaron que los recursos económicos y humanos siempre son escasos, y concentrarán sus inversiones y gastos en lo que dicte la regulación; por lo que la mayor parte del presupuesto está destinado a mitigar el riesgo de crédito, de liquidez, de mercado, legal y también el riesgo operativo, este último es el que interesa para el presente trabajo, por cuanto es el que puede sacar de funcionamiento a una cooperativa, por ejemplo debido a una caída del sistema del núcleo bancario, y porque tiene que ver en un porcentaje cercano al 50% con tecnología y la seguridad asociada.

La oportunidad identificada de las entrevistas es la necesidad y búsqueda de confianza, esta se identifica en doble sentido, esto es, desde la perspectiva de los clientes hacia la institución financiera, y desde la cooperativa hacia sus proveedores, siempre en un esquema cliente servidor; donde la confianza requerida, para optar por una empresa para realizar las inversiones en tecnología, principalmente se basa en saber gestionar el riesgo operativo, especialmente el que se puede originar desde la gestión de la calidad y de la gestión de la seguridad de la información.

Es criterio de los entrevistados que confían en un prestador de servicios que también mantiene un modelo de seguridad de la información, esto resulta totalmente entendible a la luz de los principios de la misma normativa, de cómo se va a poder apoyar a los clientes, si la misma empresa aun no es capaz de cuidar su propia información y equipamientos informáticos.

2 Análisis de resultados de la encuesta

De la pregunta 1 obtuvimos un 76,90% de personas que tienen un nivel de conocimiento adecuado de riesgos, mientras que de la pregunta 2 obtuvimos un 46,10% de los encuestados que indican haber seguido una capacitación formal en riesgos, lo que nos permite concluir que un 30 % tiene una formación empírica basada en la experiencia y los años de trabajo. Este resultado es alentador, pero aun no suficiente, frente a las exigencias regulatorias de la SEPS que cimienta su normativa en los conceptos de riesgo.

Respecto de la pregunta 3 se pudo conocer que un 69,30% de los encuestados indicaron que, sí existe una cultura del riesgo en su institución financiera, lo que es muy entendible frente al resultado de la pregunta 1 que indica que un 76,90% conocen de riesgos.

De la pregunta 4 se pudo conocer que existe un 84,50% de los encuestados que tienen un nivel adecuado respecto del riesgo operativo y únicamente un 15,5% es personal que está en etapa de formación. De este 84,50%, según la pregunta 5 todo el riesgo operativo es gestionado, un 23% de los encuestados tienen un nivel de experto, no hay nadie descalificado, esto es que tenga un conocimiento nulo sobre riesgo operativo. De estos resultados se puede apreciar que en el corto o mediano tiempo todo el personal ligado a la seguridad de la información tendrá un adecuado conocimiento del riesgo operativo, siendo esto una medida preventiva para apoyar en la minimización de ocurrencia de pérdidas económicas, por problemas en los sistemas, redes, técnicos, usuarios, procedimientos.

Los factores que influyen sobre el riesgo operativo, según la pregunta 6, se dividen en dos, los de origen tecnológicos con un 48,70% de los cuales el 25,60% corresponde a temas netamente tecnológicos y el 23,10% los derivados de los incidentes informáticos ocurridos por los ataques cibernéticos; y, por otro lado, los de

origen humano con un 51,30%, que se dividen en 19,50% correspondiente a los clientes, 16,40% a los empleados, y 15,40% a los procedimientos.

Un 61,50% de los encuestados indicaron que tienen conocimiento sobre los riesgos en seguridad de la información, y de las consecuencias que puede ocasionar un ataque informático y 69,20% indicaron que los ataques informáticos pueden provocar riesgo operativo, por lo que la diferencia del 7,7% se puede imputar a los encuestados que consideran que los ataques provocan riesgo operativo, pero no tienen conocimiento o experiencia en ataques informáticos. Cada vez es más claro el escenario de un posible ataque cibernético que ponga en riesgo la operación financiera, esto debido a que ya les ha ocurrido o conocen de algún colega que ya le ha pasado.

El 46,1% de los encuestados indica tener un plan de seguridad de la información, de éstos un 38,5% indicó que el plan de seguridad sí se alinea al giro del negocio y un 23 % que sí existe una difusión adecuada del plan de seguridad y sólo el 15,4% de los encuestados comenta que el plan se evalúa. Estos resultados demuestran un cierto grado de informalidad, debido a que los planes de seguridad que están siendo aplicados, aun no corresponden a certificaciones formales, sino más bien a crecientes intentos de mitigar los riesgos operativos producidos por ataques informáticos, con planes de seguridad autoimpuestos y de efectividad incipiente, formulados para intentar lograr un cumplimiento regulatorio.

En la pregunta 15 el 61,5 % de los encuestados indican que los incidentes de seguridad de la información que han generado un alto riesgo operativo han producido pérdidas económicas, pero conforme a las respuestas de la pregunta 14, solo el 23 % aseguran que los controles de sus planes de seguridad contribuyen a minimizar los problemas operativos, por lo que se ubica una brecha de acción, entre la materialización de los incidentes y las acciones emanadas de los controles de los planes de seguridad de la información.

En la pregunta 16 se puede apreciar que existe un conocimiento del 69,3% sobre el mejoramiento continuo y gestión de la calidad, lo cual es una cifra bastante alta, así como un 23% que está en proceso de aprendizaje o formación, por otro lado, se obtuvo un 77% que indicó que tiene alguna capacitación en mejora continua o gestión de la calidad. Estos resultados obedecen más bien a los requerimientos planteados por los usuarios de los nuevos servicios financieros, al desafío de incursionar en las transacciones digitales, al alto nivel de competencia, no solo de otras

cooperativas, sino de los bancos y de nuevas empresas que, naciendo del sector de las tecnologías de la información, empiezan a incursionar en el mundo de las finanzas.

Existe un 53,8 % que afirma tener un plan de mejora continua o gestión de la calidad operando en su cooperativa, de éste un 38,5% indican que este plan sí se alinea al objetivo del negocio, y un número similar de encuestados también aseguran que los controles de sus planes de calidad contribuyen a minimizar los problemas operativos de la organización. En este resultado sí existe un claro enfoque normativo que exige minimizar los riesgos operativos, con medidas de mejoras en sus procesos, como por ejemplo la latencia de los servicios en línea, que puede generar no solo malestar, sino también una percepción de desconfianza tanto tecnológica como de eficiencia financiera.

Una cantidad bastante alta de encuestados conforme lo revela la pregunta 22 indica que es necesario firmar un acuerdo de confidencialidad con sus proveedores, esto es del 92,3%, también con una representación bastante contundente del 84,6% se indica que es importante que los proveedores dispongan de un código de ética; adicionalmente según la pregunta 24 se conoce que un 77,9% de los encuestados consideran que sus planes de seguridad de la información o calidad deben favorecer a proveedores que cuentan con planes similares.

3 Análisis de dos estudios secundarios regionales

Para el análisis de estudios secundarios se seleccionaron dos documentos, denominados: La Evolución de Ciber-Riesgos y Seguridad de la Información, encuesta 2016 (Deloitte 2016) y el Informe Ciberseguridad 2016 ¿Estamos Preparados en América Latina y el Caribe? (BID 2016).

Se consideró la encuesta 2016 de Deloitte en virtud de ser regional, con la participación de 13 países, el 43% corresponde al sector financiero, el 40% de los entrevistados son Oficiales de la Información, el 17% seguridad informática y el 8% riesgos (Deloitte 2016, 5–7).

El 84% de los encuestados indicó que cuentan con un oficial de la información, y el 34% reportan al Gerente Informático, el 24% al Gerente de Riesgos y el 13% al Gerente General (Deloitte 2016, 16).

El 59% indicó tener una estrategia documentada de ciber-riesgos y seguridad de la información, de este un 23% indicó estar en fase de aprobación de la

documentación, y 43% restante la tiene aprobada y en operación. Solo un 13% indicó no tener nada y un 26% que están desarrollando la documentación y estiman en 12 meses tener y aprobar su estrategia de ciber-riesgo y seguridad de la información (Deloitte 2016, 18).

El principal obstáculo es la falta de recursos, el 51% de los encuestados no cuentan con los recursos para llevar adelante su gestión, un 46% indicó que tienen dificultades en el recurso humano calificado, de éste el 26% comentó que tienen falta de este recurso y el restante 20% aseveró tener dificultades para encontrar recurso humano con las capacidades requeridas (Deloitte 2016, 20).

El 61% de los encuestados indicaron tener un tablero de control, con métricas operacionales o indicadores claves KPI, que les permite conocer como impacta la seguridad en los objetivos del negocio (Deloitte 2016, 22).

La definición del presupuesto es uno de los principales factores a ser considerados. De los encuestados el 60% indicó contar con un presupuesto definido para la gestión de ciber-riesgos y seguridad de la información, y algo muy importante para el propósito de esta investigación es que el 70% está destinado a los servicios y tercerización de funciones, lo cual representa una gran oportunidad para las empresas prestadoras de servicios de seguridad (Deloitte 2016, 23).

Respecto del retorno de la inversión en seguridad de la información, ROSI, se tiene que el 40% lo calcula ya sea con reducción de riesgos o con disminución de incidentes, es decir que para este 40% la seguridad de la información dejó de ser un gasto, para el restante 60% aun lo sigue siendo (Deloitte 2016, 26).

En su informe, respecto de Ecuador, el BID (2016, 70) manifiesta que la falta de conciencia en la sociedad traza uno de los mayores retos para la seguridad ciberseguridad en el Ecuador, indica que los ciber-ataques aumentaron progresivamente durante los últimos años, lastimosamente los perjudicados no tenían presente como canalizar sus incidentes de seguridad. Con el apoyo de la academia y el sector privado se han presentado alternativas en el mejoramiento de la postura de seguridad, desde la perspectiva de la capacitación y la mejora de capacidades en evaluación para el desarrollo de software.

En este informe, el BID (2016, 71) califica al Ecuador en 5 ejes:

1. Legal, donde le otorga un nivel de 2 sobre 5, lo que indica que existen diálogos para la creación de marcos legales de seguridad cibernética sin llegar aun a establecerse, existe legislación parcial respecto a la protección

de datos personales y la privacidad, se dispone de una legislación penal básica para castigar los delitos cibernéticos, se está desarrollando derecho procesal penal para la prueba electrónica, se tiene alguna facultad de investigación para delitos relacionados a evidencias electrónicas, existen un limitado número de fiscales con capacidad de sostener una investigación por delito cibernético, y limitados jueces capaces de entender y poder emitir sentencia para delitos cibernéticos.

2. Educación, con un nivel de 2 sobre 5, que existe mercado para la educación en seguridad de la información, pero aún no hay ofertas claras que abarquen desde el nivel elemental hasta el postgrado, hay capacitación en seguridad de la información pero no es coordinada, existen incentivos y presupuesto limitado para la formación e investigación en ciberseguridad, existen programas aun limitados de capacitación, pero no se identifica transferencia de conocimientos, las juntas directivas públicas o privadas tienen algún conocimiento de los riesgos por ciber-ataques sin poder identificar la afectación que podría llegar a tener su organización.
3. Cultura y Sociedad, con un nivel de 1,5 sobre 5, que significa que algunas agencias gubernamentales han comenzado a identificar riesgos y amenazas, también empresas privadas lideres han comenzado con la identificación de prácticas de alto riesgo, ya existe alguna mentalidad de seguridad pero aun de tipo instintiva, hay campañas de sensibilización muy específicas y limitadas, persiste la preocupación por el uso de los servicios en línea, comienza a desplegarse los servicios de gobierno en línea, existe el comercio electrónico pero en su mínima expresión, empiezan a generarse o discutirse leyes sobre la privacidad y protección de datos personales;
4. Tecnologías, con una calificación de 1,5 sobre 5, que significa que se han identificado estándares de seguridad de la información con aplicación mínima, inicia un desarrollo de normas de seguridad en los procesos de contratación, existe dialogo y primeros pasos para el desarrollo de software y acreditaciones en prácticas seguras. No hay una autoridad formal de coordinación de centros de respuesta a incidentes informáticos, pero sí una gestión informal al respecto existe un equipo de respuesta nacional llamado EcuCERT con responsabilidad limitada y pocas atribuciones, ciertas amenazas se ha calificado como incidentes en el entorno nacional. Se han

identificado las empresas privadas clave para la ciberseguridad nacional sin una coordinación o autoridad gubernamental, la coordinación en incidentes de seguridad entre instituciones nacionales es casi nula, se tiene tecnología e infraestructura que permite una resiliencia limitada y reactiva, existe un registro de infraestructuras críticas nacionales sin una prelación en torno al riesgo, hay poca colaboración para la divulgación periódica de vulnerabilidades, existe conciencia para gestión de crisis sin formalizar protocolos y procedimientos; y,

5. Política y Estrategia, con una calificación de 1 sobre 5, que nos indica que no hay una estrategia nacional de seguridad, no se dispone de una entidad global para la coordinación de la seguridad cibernética, no existe una estrategia de ciberdefensa, con unas fuerzas armadas con capacidad muy limitada de resiliencia cibernética para defensa de la infraestructura crítica del país.

Comparando estos resultados con la investigación de mercado realizada, se puede observar una clara coincidencia en la madurez del sector financiero, no solo en el Ecuador, sino también en toda la región Latinoamericana; con exigencias regulatorias que protegen a los usuarios de los sistemas de banca electrónica, transferencias electrónicas, banca en línea, y principalmente sus activos de información mediante la aplicación del riesgo operativo.

4 Análisis global cruzado de resultados

De acuerdo a lo identificado por el BID[2] estamos en un nivel 2 de madurez en el desarrollo de políticas públicas de seguridad de la información, sin embargo este mismo informe puntualiza que los esfuerzos para llegar al 2 es debido a los casos individuales, como lo es la iniciativa del sector financiero, como observamos en la encuesta nacional donde tenemos un 46,1% de cooperativas que tienen un plan de seguridad de la información, un poco menos de la media dada por la encuesta de Deloitte, en la que se indica que un 59% tienen documentada una política o estrategia de seguridad de la información, por lo que se estima este número siga creciendo,

[2] Banco Interamericano de Desarrollo. Significado obtenido de la página < www.iadb.org/es> Consulta realizada en septiembre de 2018.

conforme se indicó en las entrevistas donde se mencionó que es prioritario poder llegar a cumplir a cabalidad la regulación, que exige el establecimiento de políticas de seguridad de la información y mucho mejor si es posible llegar a certificarse con alguno de los modelos internacionalmente reconocidos como lo es la ISO 27001.

El presupuesto para seguridad de la información según la encuesta de Deloitte es de un 40% como inversión y no como gasto, esto es entendible si observamos la creciente ocurrencia de incidentes de seguridad de la información. En la encuesta nacional a las cooperativas se indicó que el 61,5% han experimentado este tipo de situaciones y lo consideran la causa para la pérdida de ingresos, según las entrevistas éstas pueden ser directamente por pérdida de operatividad en los servicios, o indirectamente por pérdida de confianza en la institución financiera; también podemos considerar lo indicado por el BID donde se indica que existe una conciencia de la ocurrencia de ataques, por lo que existen incentivos y presupuesto aún limitado para la formación e investigación en ciberseguridad. Toda esta creciente tendencia hacia la inversión en temas de seguridad viene muy empujada por la regulación, según lo indicado en las entrevistas.

En educación se obtuvo una baja calificación por parte del BID otorgando al Ecuador un puntaje de 2 sobre 5 entre otras cosas por la dificultad de encontrar personal calificado en temas de seguridad de la información, por lo que hay mucha demanda y poca oferta; según lo identificado por Deloitte en su encuesta se muestra que el 51% presenta como principal obstáculo la posibilidad de recurso calificado en seguridad de la información, situación muy similar a la identificada en la encuesta nacional a las cooperativas donde se identificó un 53,8% no cuentan con alguna capacitación en seguridad de la información. Esta problemática puede ser identificada como una oportunidad ya que, al haber esta deficiencia de profesionales, la demanda de servicios tercerizados de seguridad de la información deberá seguir en aumento.

Respecto de las medidas de control desplegadas para verificación de los planes de seguridad de la información y gestión de la calidad, tenemos un resultado de la encuesta nacional de apenas 23% y 38,5%, respectivamente, mientras que en la encuesta realizada por Deloitte se obtuvo un valor del 61%, lo que deja en evidencia una brecha para Ecuador respecto del resto de Latinoamérica, esto se corrobora con lo indicado por el BID en su informe anual, donde indica un nivel de madurez muy bajo para los procesos y políticas de seguridad de la información en Ecuador, que apenas inician dialogo o primeros pasos, con casos particulares de algún desarrollo; lo que en

proyección al propósito de este trabajo de investigación, deja una oportunidad para cubrir esta brecha, con un servicio de consultoría para mejorar los controles y métricas de cumplimiento de las políticas de seguridad de la información y gestión de la calidad.

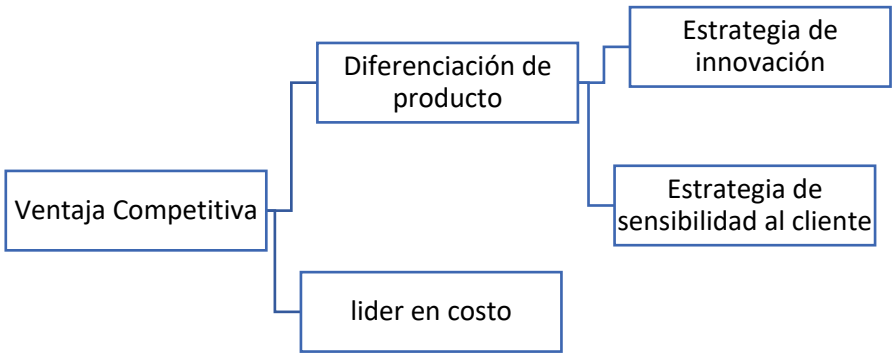
5 Diseño del plan de reorientación estratégica para Greenetics

5.1 Diagnóstico Estratégico

La estrategia de innovación corporativa se soporta sobre la clasificación del desarrollo de nuevos productos, cuya tipología se muestra en el gráfico 5, dentro de este análisis la mayor ambigüedad podría caer en la utilización de los términos innovación, invención y creatividad, indistintamente en la literatura de desarrollo de nuevos productos, tal como la sensibilidad al cliente.

Gráfico 5

Contexto de estrategias de innovación y de sensibilidad al cliente



Fuente: (Kumar y Phrommathed 2005, 6)

Elaboración propia

Para la estrategia de sensibilidad al cliente es la creatividad el factor clave, ya que se refiere más bien a la capacidad de la organización para generar nuevas ideas independientemente de cuánto se desarrollen las ideas en productos. Una organización puede ser tan creativa que tiene varias ideas planteadas por el ejecutivo y los empleados, pero no es innovadora, ya que no transforma las ideas en productos comerciales.

5.1.1 Matriz de Evaluación de Factores Internos, EFI

Para el levantamiento de la matriz de factores internos, EFI, David (2008, 149–150) nos sugiere utilizar su metodología de elaboración en cinco pasos:

1. Enumeración de factores internos clave como consecuencia de las entrevistas realizadas a tres de los profesionales que laboran en la empresa, identificándose 11 fortalezas y 14 debilidades.
2. Asignación de valor a cada factor, importancia relativa de dicho factor para tener éxito en el sector de la empresa
3. Asignación de clasificación de: 1(debilidad mayor), 2(debilidad menor), 3(fortaleza menor) y 4(fortaleza mayor)
4. Obtener el valor ponderado, resultado del producto del valor por la clasificación.
5. Sacar el total de la sumatoria de todos los valores ponderados.

Tabla 35

Valor ponderado total de factores internos clave

Factores internos clave	Valor	Clasificación	Valor ponderado
Fortalezas internas:			
Personal con adecuada capacitación	0,10	4	0,19
Profesionales con aptitud	0,10	4	0,19
Experiencia en seguridad de la información	0,10	3	0,14
Cumplimiento de los SLA	0,10	3	0,14
Satisfacción de los clientes en los servicios entregados	0,10	3	0,14
Poca burocracia interna	0,05	2	0,05
Costo de los servicios	0,15	2	0,14
Red de contactos profesionales	0,05	3	0,07
Alianzas estratégicas	0,15	3	0,21
Reputación de la empresa	0,15	2	0,14
Actitud a enfrentar nuevos retos	0,10	3	0,14
Debilidades internas:			
Falta de comunicación	0,05	1	0,02
Retardo en presentación de ofertas comerciales	0,05	1	0,02
Plan estratégico	0,10	2	0,09
Seguimiento de actividades	0,05	2	0,05
Falta de detalle en el material de capacitación	0,10	3	0,14
Falta de dirección	0,10	2	0,09
Red de contactos de alto nivel	0,05	1	0,02
Reducida cantidad de clientes en el sector financiero	0,05	1	0,02
Fuerza de ventas	0,10	1	0,05

Garantías financieras	0,05	1	0,02
Solo tiene operación en Quito	0,10	3	0,14
Indicadores financieros	0,05	2	0,05
flujo de efectivo	0,05	1	0,02
Precio de los servicios	0,10	1	0,05
Total	2,15		2,33

Fuente: Greenetics Soluciones S.A.

Elaboración propia

Un valor total ponderado de 2,33 resulta menor al promedio de 2,5 lo que indica que es una empresa, como proveedor se seguridad de la información, débil internamente.

5.1.2 Matriz de evaluación del factor externo, EFE

Para la elaboración de la matriz de factores externos, EFE, se ha considerado los pasos sugeridos por David (2008, 110).

1. Se eligieron seis oportunidades y siete amenazas, como resultado de las entrevistas realizada a los accionistas de Greenetics Soluciones.
2. Se valoró conforme la importancia de la ocurrencia.
3. Se procedió a clasificar, donde 4 es excelente, 3 sobre la media, 2 promedio, y 1 deficiente.
4. Se procede a multiplicar el valor por la clasificación y a ponderar.
5. Se realiza la sumatoria de todos los valores ponderados para obtener el total ponderado.

Tabla 36

Valor ponderado total de factores externos clave

Factores externos clave	Valor	Clasificación	Valor ponderado
Oportunidades:			
El mercado financiero popular y solidario no está muy explotado aún	5	3	0,26
Existe regulación que exige seguridad de la información	7	4	0,48
Incremento y conciencia frente a los ataques informáticos	6	2	0,21
Aumento de los riesgos de los activos en las cooperativas por ataques informáticos	3	3	0,16
Bajo conocimiento de medidas de seguridad internas de las cooperativas	5	3	0,26
Preocupación por vulnerabilidades en activos y aplicativos	7	2	0,24
Amenazas:			0,00
Legislación débil	4	1	0,07
Autoridad controladora no tan exigente	3	2	0,10
Incremento del número de empresas de seguridad de la información	5	3	0,26
Presupuestos no consideran seguridad por problemas macroeconómicos	2	2	0,07
Austeridad de gasto público para inversiones	2	2	0,07
Exceso de confianza por parte de los administradores de seguridad	4	3	0,21
Dificultad de vender productos para una empresa nueva	5	4	0,34
Total	58		2,72

Fuente: Greenetics Soluciones S.A.

Elaboración propia

Un valor total ponderado de 2,72 resulta superior al promedio de 2,5 lo que indica que es una empresa, como proveedor se seguridad de la información, mayores oportunidades que amenazas, o que pude transformar las inminentes amenazas en notorias oportunidades.

5.1.3 Matriz FODA

Para comparar y contrastar las estrategias, es muy práctico utilizar el análisis FODA, donde factores como el liderazgo en costos combinado a una base sólida operacional cimentada en una gestión de calidad total, puede verse como un factor interno con capacidad de transformarse en fortaleza (F) o debilidad (D) de una organización. Cualquier empresa que se concentre en mejorar la eficiencia de estos procesos internos convertirá esta capacidad en fortaleza. Desafortunadamente, esta capacidad tiene una limitación. Las buenas firmas no presionarán la eficiencia y la calidad más allá del punto de proporcionar reembolsos, que proporcionen un retorno favorable de la inversión; las buenas empresas reducirán los costos de manera incremental sin afectar adversamente los niveles / relaciones del servicio. Esa es la razón por la cual esta estrategia interna no tiene mucho espacio para el crecimiento de la organización. Por otro lado, la diferenciación del producto cimentado en la seguridad de la información puede verse como un atributo externo que puede clasificarse como oportunidad (O) o amenaza (A) para una empresa. Esta es la oportunidad real ilimitada para que un negocio crezca y se mantenga competitivo en el mercado. Cualquier empresa que aproveche esta oportunidad y la convierta en fortaleza disfrutará en gran medida de los resultados fijos de la inversión. (Kumar y Phrommathed 2005, 2)

Se procedió a construir la matriz FODA conforme a los pasos dados por David (2008, 201–3) esto es plasmar en los 8 cuadrantes, los 4 de factores clave (ya elaborados en las matrices EFI[3] y EFE[4]) y los cuatro de estrategia, conforme al siguiente detalle de formación de estrategias:

- Estrategia FO, fortalezas internas con oportunidades externas:

  (F1, F2, F3, F4, F5, F7, F8, F10, O4, O5, O6) Ofrecer servicios preventivos de seguridad en modalidad de outsoursing.

  (O1, O2, O3, F3, F10, F11) Diseñar un servicio de consultoría enfocado en mejorar la posición de seguridad de las Cooperativas y facilitar un cumplimiento práctico de la normativa SEPS.

[3] Evaluación del Factor Interno
[4] Evaluación del Factor Externo

(O3, O4, O5, O6, F1, F2, F3, F11, F12) Ofrecer un servicio de capacitación especializada de seguridad a las cooperativas, con talleres prácticos alineados a cumplir normativa nacional SEPS y certificaciones internacionales ISO 27015 o PSI.

- Estrategia DO, debilidades internas con oportunidades externas:

  (D1, D2, D3, D4, D6, O1, O2, O3, O4, O6) Obtener una certificación en Seguridad de la Información.

  (D1, D2, D3, D4, D6, D8, D14, O1, O2) Obtener una certificación de Gestión de la Calidad.

  (O1, O2, O3, D11, D7, D8) Generar alianzas estratégicas en otras ciudades del Ecuador enfocadas en prestas servicios y capacitaciones locales, a cooperativas fuera del entorno capitalino.

  (O1, O2, O3, D7, D8, D10, D12, D13) Generar y fortalecer alianzas estratégicas enfocadas en prestar servicios en contratos grandes a cooperativas, bancos e instituciones financieras del Estado.

  (D9, D11, D7, D2, O1, O2, O3) Aumentar la fuerza de ventas tanto de nómina, como por comisionamiento.

- Estrategia FA, fortalezas internas con amenazas externas:

  (A3, A4, A6, A7, F10, F5, F3, F2) Iniciar una campaña de mercadeo diferenciadora de la competencia.

  (F6, F7, F9, A3, A5, A7) Manejar una estrategia de precios para no perder clientes que no tienen presupuesto o que sólo contratan por precio.

  (F1, F2, F3, F4, F9, F10, A3, A5, A6, A7) Ofrecer y realizar pruebas de concepto.

- Estrategia DA, debilidades internas con amenazas externas:

  (D9, D7, D8, A3, A4, A6, A7) Entregar cursos promocionales a los potenciales clientes.

  (O1, O2, O3, O4, D13, D11, D7) Investigar la posibilidad de ingresar a mercados extranjeros.

  (D8, D9, A1, A2, A3, A4) Analizar la posibilidad de sacar otra línea de negocios como puede ser la de reciclaje de computadores.

Del resultado de construcción de la matriz FODA que se puede apreciar en el anexo 5, se obtuvieron cinco estrategias para reorientación, basadas en oportunidades y debilidades, que serán aplicadas para la reorientación estratégica planteada para la empresa Greenetics Soluciones S.A. Aquí se pueden citar los problemas identificados

en la empresa, que son: falta de formalización de su propia seguridad de la información, procesos incipientes o nulos para control de la calidad, presencia únicamente en la ciudad de Quito, falta de alianzas estratégicas para aprovechar las oportunidades del mercado de seguridad y una reducida fuerza de ventas.

5.1.4 Determinación de Código de Ética

La influencia en la confianza y decisión de compra en una institución del sector financiero popular y solidario, que puede lograr una empresa de seguridad de la información al tener un código de ética empresarial, es real, si nos sujetamos a los resultados de la pregunta 23. ¿Es importante que sus proveedores tengan un código de ética? se pudo conocer que este documento si genera valor para los profesionales encuestados de las instituciones financieras, con un 86,4% de resultados afirmativos, esto quiere decir que contar con este documento es necesario, pero esto solo significará un adicional positivo para la toma de valor conforme se pudo indagar en las entrevistas, este tipo de iniciativa agrega valor, pero por sí solo no es el factor preponderante para la toma de decisión.

Por lo expresado se ha incluido como parte de la reorientación estratégica un modelo de código de ética para la empresa Greenetics, que consta en el anexo 6.

5.2 Incorporación de la normativa ISO 9001

La empresa Greenetics Soluciones S.A. incorporará una filosofía de mejora continua y una metodología de gestión de la calidad, estructurada en base a la norma ISO 9001, considerando los resultados de la pregunta 24, donde se colige que es casi un requisito para poder entrar al sector financiero de economía popular y solidaria, que la empresa cuente con una normativa para la gestión de la calidad.

Conforme lo indica Heras (2018, 8) la difusión exitosa de la ISO 9001 podría estar relacionada con el ímpetu básico del proceso de globalización de las economías occidentales, las cadenas de suministro mundiales que se extienden y el papel crucial de las empresas transnacionales, como modelo de ejemplo y generación de una cultura de la calidad.

En el entorno económico actual, en el cual Grenetics debe afrontar la externalización y reubicación de las actividades hacia el sector financiero, hace a la

gestión de calidad un elemento estratégico clave dentro de las cadenas de servicios globales de las cooperativas, por lo que es necesario fomentar un cierto nivel de homogeneidad de los sistemas de gestión que se manejan en Greenetics para favorecer el desarrollo de dichos procesos, y estándares pueden ayudar a lograr este objetivo.

La generalización de los estándares de los sistemas de gestión en todo el mundo también ha sido percibida por instituciones internacionales como la Unión Europea y la Organización Mundial del Comercio, como una forma de reducir las barreras técnicas al comercio, facilitar las transacciones comerciales y reforzar el proceso de globalización (Heras-Saizarbitoria 2018, 8).

5.2.1 Contexto de la Organización

Para que Greenetics pueda incorporar una filosofía de calidad total y mejora continua, es necesario identificar cuál es la realidad de la empresa, conocer sus problemas latentes, conocer y mapear las partes interesadas con sus expectativas y necesidades, a fin de poder redirigir los productos y servicios al cumplimiento regulatorio de sus clientes, en este caso al exigido por la SEPS a las cooperativas de ahorro y crédito. En el presente estudio se pudo identificar los principales problemas de Greenetics, que fueron plasmados en las matrices de evaluación de factores internos y externos, sin embargo, dentro de un proceso de certificación esta información deberá ser ampliada con la respectiva auditoría interna que deberá realizar la empresa certificadora.

Comprender el contexto de una organización como Greenetics, es ahora un requerimiento obligatorio, una vez que se ha decidido adoptar oficialmente la norma ISO 9001:2015 y, cuando se desarrolla un sistema de gestión de la calidad (SGC), se requiere identificar, analizar y comprender el entorno empresarial en el que la organización desarrolla su actividad y se da cuenta de su producto (Abuhav 2017, 7).

En el proceso de certificación es necesario que Greenetics determine los problemas externos e internos relevantes para su propósito y su dirección estratégica. Una vez que se haya implementado la norma ISO 9001, se debe monitorear y revisar la información sobre los problemas externos e internos que afectan su capacidad para lograr los resultados esperados de su sistema de gestión de calidad (Dentch 2017, 18).

Greenetics debe determinar las partes interesadas que son relevantes para su sistema de gestión de calidad. Del presente estudio se identificaron otras cooperativas,

gremios de cooperativas, fabricantes, proveedores, socios comerciales, Superintendencia de Bancos, Superintendencia de Economía Popular y Solidaria, otras empresas de seguridad, delincuentes cibernéticos, usuarios de servicios en línea.

La gerencia de operaciones debe monitorear y revisar la información sobre las partes interesadas y su efecto potencial sobre la capacidad de Greenetics para proporcionar consistentemente productos y servicios que cumplan con los requisitos reglamentarios y legales del cliente (Dentch 2017, 18).

5.2.2 Liderazgo

Para la gerencia general de Greenetics es clara la necesidad de apoyar el proceso de implementación del sistema de gestión de calidad SGC, con una política documentada de inclusión de todos los empleados en el concepto de calidad, e incluyendo la delegación de autoridad y responsabilidades, que permitan conducir a la empresa al establecimiento del SGC.

El éxito de implementar un sistema de gestión de calidad SGC depende del compromiso de la alta dirección. El liderazgo en todos los niveles organizacionales debe crear un entorno que inicie y promueva condiciones en las que los empleados sientan el compromiso de lograr los objetivos de Greenetics (Abuhav 2017, 39).

La gerencia general debe establecer una política de calidad que sea apropiada para el propósito y el contexto de Greenetics, que respalde su dirección estratégica y que mediante la gerencia de planificación pueda ser implementada y mantenida en el tiempo. La política de calidad estará disponible y se mantendrá como información documentada y se comunicará, comprenderá y aplicará dentro de la organización (Dentch 2017, 27).

La gerencia general se asegurará mediante la gerencia de operaciones, que las responsabilidades y autoridades para los roles relevantes se asignen y se comuniquen dentro de Greenetics, se pone énfasis en la necesidad de delegar funciones para cumplimiento del SGC (Dentch 2017, 30).

5.2.3 Planeación

La planeación de Greenetics se basará en los principios de mejora continua del SGC, incluirá la esquematización del riesgo para prevención de la información que se

maneja de los clientes y buscar que en los cambios que se están proponiendo se consideren las oportunidades y consecuencias que se pueden generar, principalmente desde la perspectiva del sector financiero popular y solidario.

El pensamiento basado en el riesgo sugiere a Greenetics el buscar oportunidades, abordar riesgos identificados y proponer acciones para desarrollar esas oportunidades identificadas o para mitigar o eliminar los riesgos no aprovechables. El pensamiento basado en el riesgo es en realidad un desarrollo y una ampliación del conocido concepto de "acción preventiva". Las organizaciones, y en este caso Greenetics, deben migrar de la acción preventiva al pensamiento basado en el riesgo (Abuhav 2017, 67).

Este concepto indica que los cambios producen oportunidades y consecuencias imprevistas; es decir, cuando Greenetics analiza y actúa con anticipación para abordar los cambios que pueden afectar sus objetivos, las expectativas de las partes interesadas o los requisitos del producto. Por lo tanto, antes de crear un cambio, se debe identificar y evaluar los riesgos y oportunidades asociados (Abuhav 2017, 69).

La empresa Greenetics determinará la necesidad de cambios en función de las necesidades de los clientes y de la mejora interna, considerando siempre el sistema de gestión de la calidad SGC, esto significa que todos los cambios se llevarán a cabo de forma planificada. Greenetics deberá considerar: El propósito de los cambios y sus posibles consecuencias, la integridad del sistema de gestión de calidad, la disponibilidad de recursos y la asignación o reasignación de responsabilidades y autoridades (Dentch 2017, 39).

5.2.4 Soporte

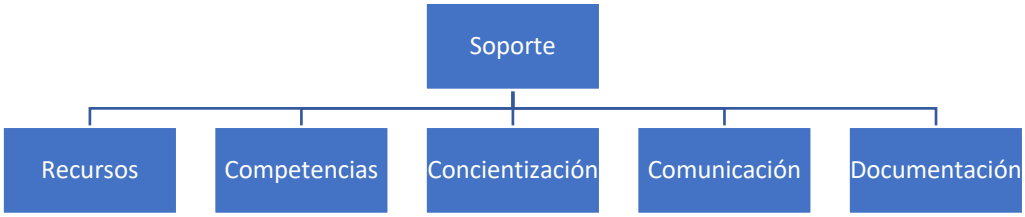
Los recursos con los que cuenta Greenetics son escasos y se consideran herramientas de soporte para que el SGC alcance los objetivos planteados por Greenetics. La norma enfatiza las implicaciones de no cumplir con los requisitos de la administración, esto significa que la determinación y definición de los recursos debe estar alineada con los objetivos del SGC y los recursos deben ser los adecuados.

La idoneidad de los recursos otorgados por la gerencia general debe ser evaluada, de acuerdo con una escala de medición, ya que la norma espera poder medir la compatibilidad de los recursos asignados por Greenetics con las expectativas del SGC. Además, las actividades subcontratadas se consideran recursos externos que

deben definirse y, posteriormente, controlarse. Por otro lado, el soporte de la concienciación es cada vez más importante ya que aumenta la motivación y la devoción de los empleados (Abuhav 2017, 101).

Gráfico 6

Los cinco niveles de soporte del SGC



Fuente: (Dentch 2017, 42)

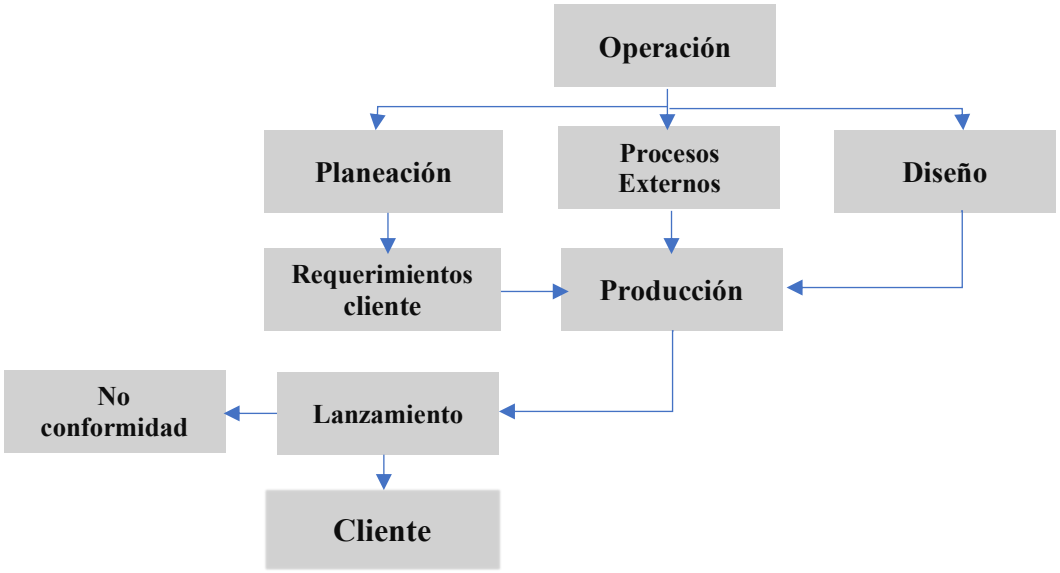
Elaboración propia

5.2.5 Operación

La planificación y el control operativos en Greenetics iniciarán con la planificación maestra para la realización de productos o servicios considerando los requerimientos del cliente, con los objetivos de planificar, realizar, controlar, dirigir, guiar e instruir a todos los participantes sobre las diferentes funciones y roles involucrados en la realización de un servicio: cómo administrar el diseño y desarrollo, cómo prepararse para la realización, cómo identificar y localizar los recursos apropiados, qué actividades son necesarias, qué controles se deben aplicar, qué información documentada es necesaria, cómo se verifican o validan los resultados, y cuáles evidencias se esperan (Abuhav 2017, 189).

Gráfico 7

Descripción de la operación del SGC



Fuente: (Dentch 2017, 55)

Elaboración propia

5.2.6 Evaluación del desempeño

El gerente de operaciones de Greenetics debe determinar los métodos para el monitoreo, la medición, el análisis y la evaluación de la efectividad del sistema de gestión de la calidad y retener la información documentada apropiada como evidencia de los resultados (Dentch 2017, 81).

La auditoría interna es una herramienta efectiva que se utilizará para la autoevaluación de Greenetics y para determinar en qué medida se cumplen los requisitos del SGC. Los resultados de la auditoría (los hallazgos de la auditoría) deberán demostrar la efectividad del SGC e identificar las no conformidades y las oportunidades de mejora (Abuhav 2017, 375).

La revisión gerencial se incorpora a las actividades de la gerencia de Greenetics, esta es una herramienta de gestión periódica en manos de la alta dirección para evaluar el SGC. Es uno de los tres métodos dictados por el estándar para monitorear el SGC y evaluar su desempeño y eficacia. La revisión gerencial es una actividad que se realizará trimestralmente con una reunión extraordinaria de la junta de accionistas, en la que los representantes de la alta dirección recibirán los datos e información sobre el desempeño del SGC (Abuhav 2017, 386).

5.2.7 Mejoramiento

El mejoramiento para Greenetics dentro del Estándar ISO 9001 es un concepto permanente, de contacto con el cliente, por medios principalmente digitales, pero también físicos, que impulsará a Greenetics a cumplir con los requisitos del cliente y mejorar el logro de los objetivos de calidad y la satisfacción del cliente. La mejora significa, de alguna manera, encontrar los parámetros que afectan el logro de las metas y someterlas al cambio. El desafío es identificar los procesos específicos que tienen el mayor efecto en la conformidad de los servicios para la satisfacción del cliente (Abuhav 2017, 397). Por ejemplo en el servicio de cursos y talleres, si se hace una exhaustiva evaluación de cada curso, esto es: de los instructores, del material entregado, del cumplimiento del temario, de la efectividad de las prácticas y de las instalaciones, toda esta información de retorno entregada por los alumnos, permiten mejorar permanentemente este servicio y mantenerse vigente en el tiempo; esta buena práctica deberá extenderse a otros servicios y productos ofertados por Greenetics, para cumplir el acápite de mejoramiento del estándar de gestión de la calidad.

Greenetics debe determinar y seleccionar oportunidades para mejorar el rendimiento y la efectividad del sistema de gestión de calidad e implementar las acciones necesarias para aumentar la satisfacción del cliente, para incluir: mejoras en los productos y servicios que permitan cumplir con los requisitos y abordar las necesidades y expectativas. Corregir, prevenir o reducir el efecto no deseado (Dentch 2017, 92). Muchas de las oportunidades fueron identificadas en el presente estudio, tales como: El mercado financiero popular y solidario no está muy explotado, existe regulación que exige seguridad de la información, hay un incremento y conciencia frente a los ataques informáticos, existe un aumento del riesgo en los activos de las cooperativas por ataques informáticos, persiste un bajo conocimiento de medidas de seguridad internas de las cooperativas y crece la preocupación por vulnerabilidades en activos y aplicativos.

5.3 Incorporación del Modelo de Seguridad de la Información

5.3.1 Contexto de la Organización

La naturaleza de las amenazas a la seguridad de la información siempre está cambiando, tanto la tecnología y el contexto dentro del cual una organización mantiene su información, están en constante transformación, este es un factor que Greenetics tomará siempre en cuenta antes de hacer un levantamiento de información previo a la prestación de un servicio.

El oficial de seguridad de la información de Greenetics, al momento de hacer la evaluación de brechas de seguridad, o al analizar el estado de salud de la red del cliente, deberá ser capaz de responder a las nuevas amenazas, encontrar y proteger las vulnerabilidades en las nuevas tecnologías que la organización desea implementar y poder validar la necesidad de cumplimiento regulatorio, para mejorar la ventaja competitiva de la empresa (Calder y Watkins 2008, 75). Esta capacidad se logra con el uso de herramientas como la inteligencia de amenazas, la gestión y monitoreo de vulnerabilidades, la inteligencia artificial, simulación de brechas y mejoras en los sistemas de autentificación y encriptación de información.

5.3.2 Liderazgo

La política de seguridad de la información a ser implantada en Greenetics deberá proporcionar orientación general sobre quién es responsable de qué activo de seguridad de la información, por lo que es probable que esta orientación sea muy amplia y deba ser referenciada a la criticidad de acuerdo con el nivel de riesgo que presenta cada uno de los activos.

Por lo que, Greenetics deberá definir claramente quién es responsable de qué proceso de seguridad y/o activo de información y puede tener que ver también las responsabilidades geográficas o del sitio (Calder y Watkins 2008, 58).

Para la gerencia de Greenetics es evidente el requerimiento de la norma para facilitar toda actividad del proceso de implementación del sistema de gestión de seguridad de la información SGSI, con una política por escrito, con inclusión de todos los empleados en el concepto de la seguridad de la información, e incluyendo la

delegación de autoridad y responsabilidades, que permitan conducir a la empresa al establecimiento del SGSI.

5.3.3 Planeación

El estándar requiere que Greenetics controle sus demandas de capacidad operativa y luego haga proyecciones de los niveles de actividad comercial, por lo tanto, deberá existir un vínculo evidente y un equilibrio entre esta actividad y el ciclo anual de planificación comercial.

Una de las tendencias que Greenetics debe considerar en la prestación de los servicios de seguridad a sus clientes es con respecto del aumento en la actividad comercial, por lo tanto, en el procesamiento de transacciones, el aumento en el número de personal, y por lo tanto en el número de estaciones de trabajo y otras instalaciones.

Todo esto debería permitir a los administradores de redes y webmasters de Greenetics, en coordinación con los profesionales de la seguridad y de tecnologías de la información de los clientes, el poder identificar y evitar potenciales cuellos de botella que podrían amenazar la seguridad del sistema o la disponibilidad de recursos o datos de la red o del sistema (Calder y Watkins 2008, 176).

5.3.4 Soporte

Para un adecuado soporte, la norma considera necesario que Greenetics destine especial atención a cinco ejes principales que son: Recursos, Competencias, Concientización, Comunicación y Documentación.

Para el soporte Greenetics deberá considerar dos tipos de controles: seguridad de los archivos del sistema y la seguridad en los procesos de desarrollo y soporte. El objetivo del primero es garantizar que los proyectos de TI y las actividades de soporte se realicen de forma segura (y sin exponer datos confidenciales en un entorno de prueba), mientras que el objetivo del segundo es mantener la seguridad del software y la información del sistema de aplicación. No existe una relación estructural profunda entre estos dos controles (Calder y Watkins 2008, 282).

5.3.5 Operación

El estándar requiere que Greenetics documente los procedimientos operativos que se identificaron como necesarios en la política de seguridad para que sobre las necesidades identificadas en el cliente puedan pasar a un estado de producción, asegurando un cumplimiento normativo del cliente frente a sus entidades de control.

Los principios de control de documentos de ISO 9001 son aplicables y concordantes a los documentos de la ISO 27001, y todos los procedimientos operativos que forman parte del SGSI de la organización deben tratarse de acuerdo con estos requisitos, incluida la aprobación de la gerencia correspondiente antes de proceder al lanzamiento del servicio o sus modificaciones (Calder y Watkins 2008, 167).

5.3.6 Evaluación del Desempeño

Todos los principios y procedimientos establecidos por Greenetics para la evaluación del rendimiento operativo se mantienen válidos cuando se aplican a la seguridad de la información y a la medición de la eficacia del Sistema Gestor de Seguridad de la Información, SGSI y sus controles.

De la experiencia en la prestación de servicios de seguridad por parte de la empresa Greenetics se puede mencionar que: los reportes negativos probablemente den lugar a medidas defectuosas; el monitoreo automatizado es preferible a los arreglos manuales; el aspecto exacto que se mide debe alinearse con el principal objetivo; y la integridad de las medidas o estadísticas que se producen es para aumentar la importancia, ya que las decisiones de gestión probablemente se basen en esta información (Calder y Watkins 2008, 100).

5.3.7 Mejoramiento

Para la mejora del SGSI de Greenetics se considera la integración en componentes específicos necesarios y partir del enfoque de mejora continua por sus siglas en ingles PDCA, como objetivo final de lograr un sistema unificado de gestión, que además de calidad y seguridad, en un futuro podría incorporar: salud, ambiental y negocio.

Los requisitos de acción correctiva se cumplen mediante un plan efectivo de auditoría del SGSI a ser implantado dentro de la empresa Greenetics, la revisión competente de las no conformidades como parte de la responsabilidad del gerente de seguridad de la información, los procedimientos de respuesta a incidentes y la documentación relacionada. La prevención es siempre mejor que la corrección y, el gerente de seguridad de la información debe tener una responsabilidad específica en términos de planificación e implementación de la acción preventiva (Calder y Watkins 2008, 47).

5.4 Definición de Misión y Valores

La misión se redefinirá en base a las estrategias identificadas de los análisis de las matrices EFI, EFE y FODA, considerando la alineación de los objetivos a ser alcanzados, con suficiente amplitud para atraer diferentes grupos de interés, descripción de lo que es la empresa, el propósito, la filosofía y el servicio prestado en general.

Misión redefinida y construida con personal de la empresa Greenetics Soluciones S.A.:

Greenetics es el aliado estratégico en seguridad de la información, que contribuye al perfeccionamiento y cumplimiento regulatorio de sus clientes, proporcionando servicios y herramientas innovadoras que garantizan la operación ininterrumpida, agregando valor y generando confianza para ganar su lealtad.

A partir de la declaración de la nueva misión, con la participación del personal de Greenetics se consideraron y aprobaron cinco valores con sus respectivas definiciones, que ayudarán a su cumplimiento:

1. Responsabilidad: Involucrar al personal en el cumplimiento de sus funciones, y del cumplimiento para los clientes.
2. Trabajo en equipo: Integrar la comunicación y la participación de los equipos de trabajo con las diferentes áreas de la empresa a fin de obtener los objetivos deseados.
3. Proactividad: Realizar acciones favorables ante posibles eventos que puedan influir en el cumplimiento de los objetivos de la Empresa.
4. Respeto: Observar los derechos de las personas y del medio ambiente.

5. Lealtad: Fiel cumplimiento de la normativa legal y los valores de la institución bajo principios de legalidad, verdad y honorabilidad.

5.5 Definición de Visión y Objetivos Estratégicos

En base a la nueva misión, con el concurso del personal de Greenetics se procede a redefinir la visión de la empresa Greenetics Soluciones S.A., con la pregunta ¿Qué queremos llegar a ser?

Ser un referente en el sector de seguridad de la información, con presencia nacional, con reconocimiento internacional, por nuestro permanente empeño de mejora continua; logrando posiciones de excelencia en ventas de soluciones de seguridad digital, a los precios más competitivos del mercado, con una gestión orientada a los clientes y a su cumplimento regulatorio.

Los objetivos estratégicos para lograr la reorientación estratégica planteada son los siguientes:

Lograr el 20 % del mercado de la seguridad de la información en el sector de cooperativas de nivel 2, esto significa que para finales del año 2019 se tendrá 8 clientes nuevos del sector financiero popular y solidario de nivel 2.

Lograr el 12% de mercado de la seguridad de la información en el sector de cooperativas de nivel 1, esto significa que para finales del año 2019 se tendrán 3 clientes nuevos del sector financiero popular y solidario de nivel 1.

Lograr un aumento de los ingresos por cursos en un 10%, con la incorporación de al menos un taller teórico - práctico diseñado para que las cooperativas de ahorro y crédito logren su cumplimiento regulatorio, con énfasis en seguridad de la información, riesgos operativos, plan de continuidad del negocio y cumplimiento de la regulación de la SEPS.

5.6 Estrategia Organizacional

Se propone una estructura organizativa funcional basada en procesos, en la cual se pretende tener una estrecha cadena de mando a través del Consejo Directivo, conformado por el gerente general y las gerencias con responsabilidades definidas y distribuidas categóricamente; que permita tomar decisiones rápidas, agregar valor a los procesos, optimizar relaciones comerciales, lograr un manejo transparente de la

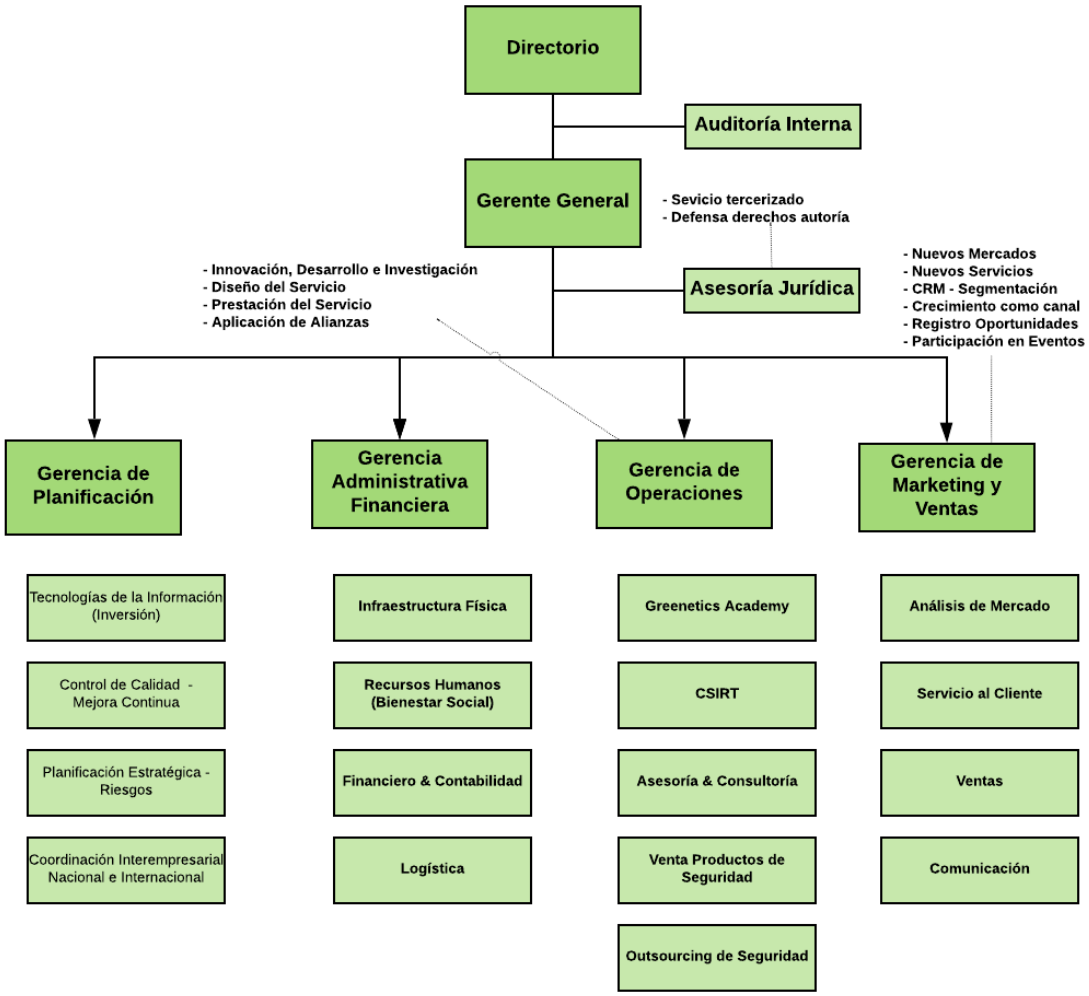
información, difundir objetivamente el giro del negocio, mejorar la comunicación y motivación de las personas.

El detalle de las áreas funcionales de la nueva estructura de la empresa se muestra en el gráfico 8, con la finalidad de identificar la interacción y distribución de funciones dentro de los procesos.

- Directorio: Aprobar los proyectos y planes empresariales, tales como el de inversiones, también las alianzas estratégicas y la contratación de personal.
- Gerencia General o representante legal: Administra la empresa a través de los planes aprobados, entre estos los sistemas de gestión de calidad y seguridad.
- Gerencia de Planificación: Elabora los planes y proyectos de la empresa, estará a cargo de la elaboración de los sistemas gestor de calidad y de seguridad.
- Gerencia Financiera Administrativa: Servirá de apoyo para la implementación del SGSI y del SGC, con soporte de recursos, logística.
- Gerencia de Operaciones: Es la encargada de implementar el SGSI y el SGC, así como de las alianzas estratégicas.
- Gerencia de Marketing y Ventas: dentro del plan de mejora continua son de vital importancia para traer la percepción del cliente respecto de los servicios prestados.
- Auditoría Interna: Supervisar los procesos de auditoría interna de SGSI y SGC.
- Asesoría Jurídica: Validará jurídicamente todo lo actuado para la implementación de los planes, proyectos y metodologías.

Gráfico 8

Detalle de la nueva estructura



Fuente: (Greenetics 2018)

Elaboración propia

5.6.1 Estrategia genérica

Se ha escogido una estrategia genérica de enfoque, buscando la oportunidad en el segmento popular y solidario, del sector financiero, que aún no tiene un tamaño suficiente en materia de seguridad de la información, sin embargo, cuenta con un inmenso potencial de crecimiento, que aún no ha sido identificado por otros competidores más grandes.

Conforme lo indicado por David (2008, 176) todas la empresas siguen una estrategia de diferenciación intrínseca, en este caso Greenetics buscará el factor de la diferenciación a través de fomentar el factor confianza, para lo cual se iniciará con la aplicación de un código de ética, y dos certificaciones internacionales, una en seguridad de la información y otra en calidad total, a fin de poder ser considerado el aliado estratégico de las cooperativas.

Para aplicar la estrategia de enfoque se aprovechará que las cooperativas de ahorro y crédito tienen necesidades y requerimientos específicos, como el cumplimiento regulatorio expedido por la SEPS, y que aún no se evidencia una presencia de competidores en este segmento del mercado.

Muchos competidores podrán luego identificar al mercado de cooperativas de ahorro y crédito, lo cual representa un factor de riesgo latente, por lo que aquí entra en juego el poder logrado con los diferenciadores que generan confianza, sumado a la fidelización que se puede lograr con una adecuada aplicación de un modelo de calidad total.

También se mejorarán las fortalezas de Greenetics, esto es: Personal con adecuada capacitación, aptitud profesional, actitud a enfrentar nuevos retos y experiencia en seguridad de la información; reputación de la empresa, por satisfacción de los clientes en los servicios entregados, cumplimiento de los SLA[5], servicios ágiles, costo adecuado de los servicios, adecuada red de contactos profesionales y colaboradores externos reconocidos.

5.6.2 Estrategia específica

Greenetics es una empresa que persigue estrategias innovadoras y sensibles al cliente para desarrollo de nuevos productos, por lo que busca tener más éxito en los negocios que las empresas que se dedican a un solo enfoque (Kumar y Phrommathed 2005, 109–14).

De acuerdo con esta hipótesis, demostrada por Kumar, es necesario que las estrategias a ser implementadas sean innovadoras y sensibles, por lo que finalmente

[5] Service Level Agreement, es un acuerdo de nivel de servicio para cumplir con los clientes, normalmente adjunto al contrato de prestación del servicio. Definición tomada de <https://www.ibm.com/support/knowledgecenter/es/SSKVFR_7.6.1/com.ibm.spr.doc/sla_spr/c_sla_application.html> Consulta realizada en septiembre de 2018.

las estrategias específicas a ser adoptadas por Greenetics serán de reorientación, de diferenciación y ofensivas, se utilizarán 9 de las estrategias obtenidas, todas como resultado de los análisis EFI, EFE y FODA.

Para Greenetics se iniciará con estrategias de reorientación a fin de fortalecer las debilidades, pero aprovechando las oportunidades que se evidencian del sector financiero popular y solidario: 1) Obtener una certificación de Gestión de la Calidad soportada en la norma ISO 9001; 2) Obtener una certificación en Seguridad de la Información de acuerdo con la norma ISO 27001; 3) Generar alianzas estratégicas en otras ciudades del Ecuador enfocadas en prestar servicios y capacitaciones locales, a cooperativas fuera del entorno capitalino. 4) Generar y fortalecer alianzas estratégicas enfocadas en prestar servicios en contratos grandes a cooperativas, bancos e instituciones financieras del estado. 5) Aumentar la fuerza de ventas tanto de nómina, como por comisionamiento, con el propósito de visitar cooperativas de ahorro.

Dos estrategias de diferenciación, para posicionar las nuevas fortalezas de Greenetics. 6) Iniciar una campaña diferenciadora de mercadeo digital, a fin de posicionar a la empresa como un referente de la seguridad de la información en cooperativas; 7) Manejar una estrategia de precios para no perder cooperativas de ahorro y crédito que no tienen presupuesto o que sólo contratan por precio y para cumplir con la regulación de la SEPS;

Finalmente, se ha considerado para Greenetics, dos estrategias ofensivas, para aprovechar las fortalezas y las nuevas capacidades desarrolladas en las estrategias anteriores. 8) Diseñar un servicio de consultoría enfocado en mejorar la posición de seguridad de las Cooperativas y facilitar un cumplimiento práctico de la normativa SEPS. 9) Ofrecer un servicio de capacitación especializada de seguridad a las cooperativas, con talleres prácticos lineados a cumplir normativa nacional SEPS y certificaciones internacionales ISO 27015 o PSI.

5.6.3 Tácticas y acciones

Para la primera Estrategia Específica, obtener una certificación de Gestión de la Calidad soportada en la norma ISO 9001, se han considerado 4 tácticas o planes de acción, dentro de estos se tienen 19 acciones prioritarias asociadas:

1. Táctica o Plan de Acción 1: Preparación empresarial

- E1T1.1: Obtener física o digitalmente la Norma ISO 9001:2015, y ponerla en un repositorio que pueda ser compartido y accedido por todos los profesionales que estarán envueltos en la implementación de esta normativa.
- E1T1.2: Revisar procesos y procedimientos actuales, desde el accionar del día a día, a manera de una auditoría interna para levantamiento de información.
- E1T1.3: Validar si estos procesos y procedimientos están documentados, si no lo están se deberá escribirlos, conforme se vienen desarrollando de manera ad-hoc.
- E1T1.4: Validar si estos procesos y procedimientos se cumplen, ya sea que estén por escrito o que sea producto de la práctica diaria y desarrollo empírico.

2. Táctica o Plan de Acción 2: Preparación Recurso Humano
    - E1T2.1: Certificar a los profesionales que serán encargados de la implementación de la norma ISO 9001, aquí lo recomendable es que, tanto al gerente de planificación, como al gerente de operaciones, se les de una capacitación a nivel de certificación profesional.
    - E1T2.2: Realizar una evaluación de clima laboral, enfocada en conocer qué tan proclive está el personal de la empresa para afrontar cambios estructurales y de corto plazo.
    - E1T2.3: Realizar un coaching para motivar al personal y alinearlo al nuevo reto de la empresa, tendiente a lograr la adopción de las nuevas normativas considerando el accionar de la empresa y las necesidades de los clientes.
    - E1T2.4: Charlas de los profesionales internos certificado, al resto del personal de la empresa, con talleres dinámicos y que respondan a los intereses de la empresa en el mediano y corto plazo.
3. Táctica o Plan de Acción 3: Gestión Recursos.
    - E1T3.1: Buscar una empresa para realizar la auditoría de certificación, considerando experiencia y mejores costos.
    - E1T3.2 Realizar un levantamiento interno de cuánto costará la implementación de la ISO 9001.
    - E1T3:3. Reservar el recurso humano, en horas hombre, que será utilizado en el proceso de certificación ISO 9001.
    - E1T3.4: Determinar los gastos necesarios para cubrir los gastos en insumos y logística necesarios para completar la auditoria de certificación en ISO 9001.

4. Táctica o Plan de Acción 4: Implantación
    - E1T4.1: Identificar, analizar y comprender el contexto de la organización para que la normativa se pueda alinear a la operación de Greenetics.
    - E1T4.2: Plasmar el compromiso de la alta gerencia en un documento por escrito, que certifique su aprobación y respaldo.
    - E1T4.3: Planificar los cambios, en base a la matriz de riesgos y al esquema de mejora continua, en un plan de implementación de SGC.
    - E1T4.4: Determinar los soportes necesarios: Recursos, competencias, concientización, comunicación y documentación.
    - E1T4.5: Lanzar la operación del SGC, en un evento formal interno y de ser posible también externo para dar realce es este importante esfuerzo por parte de todos los que forman la empresa Greenetics.
    - E1T4.6: Determinar los métodos para el monitoreo, la medición, el análisis y la evaluación del SGC.
    - E1T4.7: Mejora continua del SGC, involucrando como responsable principal a la gerencia de marketing y ventas de Greenetics.

Para la segunda Estrategia Específica, obtener una certificación de Gestión de la Seguridad de la Información soportada en la norma ISO 27001, se ha considerado 4 tácticas o planes de acción, dentro de estos se tienen 24 acciones prioritarias asociadas:

1. Táctica o Plan de Acción 1: Preparación empresarial
    - E2T1.1: Obtener la Norma ISO 27001:2018 y ponerla en un repositorio que pueda ser compartido y accedido por todos los profesionales que estarán envueltos en la implementación de esta normativa.
    - E1T1.2: Revisar Políticas de seguridad de la información, tanto administrativas como operacionales.
    - E2T3.3: Revisar procesos y procedimientos de seguridad de la información desde el accionar diario, a manera de una auditoría interna para levantamiento de información.
    - E2T1.4: Elaborar la matriz de riesgos, incluyendo todos los activos de la información, pero también a los elementos relacionados hacia las posibles necesidades de los clientes.

- E2T1.5: Validar si políticas, procesos y procedimientos están documentados, si no lo están deberán ser escritos, conforme se vienen desarrollando de manera intuitiva.
- E1T1.6: Validar si estos procesos y procedimientos se cumplen, ya sea que estén por escrito o que sean producto de la práctica cotidiana y aprendizaje experimental.

2. Táctica o Plan de Acción 2: Preparación Recurso Humano
   - E2T2.1: Certificar el profesional que será encargado de la implementación como lead implementor ISO 27001, en el caso de Greenetics ya se cuenta con tres implementadores lideres ISO 27001, por lo que esta actividad ya estaría cumplida de antemano.
   - E2T2.2: Realizar una evaluación de clima laboral, enfocada en conocer que tan propenso está el personal de Greenetics para afrontar cambios significativos en la esencia de sus servicios.
   - E2T2.3: Realizar un coaching para motivar al personal y alinearlo al nuevo reto de la empresa, evitar el bloqueo al cambio.
   - E2T2.4: Charlas del profesional certificado, al resto del personal de la empresa para la implementación de la ISO 27001, las cuales deberán ser práctica y con talleres, más que teóricas, deben llamar a la acción.
   - E2T2.5: Programa de concientización en seguridad de la información a todos los empleados.
   - E1T2.6: Firma de Acuerdos de Confidencialidad NDA con todos los empleados de Greenetics.
3. Táctica o Plan de Acción 3: Gestión Recursos
   - E2T3.1: Buscar una empresa para realizar la auditoría de certificación, considerando experiencia y mejores costos.
   - E2T3.2 Realizar un levantamiento de cuánto costará la implementación de la norma ISO 27001, con el respectivo mapeo hacia la ISO 9001, por actividades comunes.

- E2T3:3. Reservar el recurso humano que será utilizado en el proceso de certificación ISO 27001, levantar una matriz RACI[6] para asignación de responsabilidades.
- E2T3.4: Determinar los gastos para cubrir los gastos en insumos y logística para la auditoria ISO 27001.
- E2T3.5: Adquirir un software de automatización tal como el Software 'ISOTools Securitiy'[7].

4. Táctica o Plan de Acción 4: Implantación
   - E2T4.1: Identificar, analizar y comprender el contexto de la organización para que la normativa se pueda alinear a la operación de Greenetics.
   - E2T4.2: Plasmar el compromiso de la alta gerencia en un documento compromiso suscrito.
   - E1T4.3: Planificar los cambios, elaborar el Sistema Gestor de Seguridad de la Información SGSI.
   - E2T4.4: Determinar los soportes necesarios: Recursos, competencias, concientización, comunicación y documentación.
   - E1T4.5: Lanzar la operación del SGSI, considerando la nueva matriz de riesgos
   - E2T4.6: Determinar los métodos para el monitoreo, la medición, el análisis y la evaluación del SGSI.
   - E2T4.7: Mejora continua del SGSI con la operatividad del 'ISOTools Security'.

Las tácticas y planes de acción para las estrategias 3, 4, 5, 6, 7, 8 y 9, se encuentran en el anexo 7.

5.6.4 Indicadores

[6] Matriz Raci hace referencia directa a sus elementos: R: Responsible (responsable), Es el rol más empleado en la Matriz de Raci. Señala a la persona que se encarga de realizar una tarea o acción específica. A: Accountable (persona a cargo): Se trata de la persona que tiene la responsabilidad de que las tareas estén hechas. No necesariamente debe hacerlas él mismo; puede delegarlas en otros, lo cual no le exime de su responsabilidad hacia el grueso del proyecto. C: Consulted (consultor): Son todas aquellas personas a las que se consultan datos o información relacionada con la ejecución de las tareas de un proceso. I: Informed (informador): En este caso, son las personas a las que se informa de todo lo que sucede durante la ejecución de las labores previstas. Definición obtenida de https://www.obs-edu.com/int/blog-project-management/herramientas-esenciales/cual-es-la-funcion-principal-de-la-matriz-raci Consulta realizada en agosto de 2018.

[7] <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>. Consulta realizada en junio de 2018

Se ha considerado los indicadores para cumplimiento y mejora continua de los objetivos estratégicos, para cada indicador se abre una ficha de clasificación, que incluye: la definición del indicador, la forma de cálculo, el responsable, frecuencia de levantamiento, finalidad, fuente de información, nivel del reporte, proceso dentro de la cadena de valor, especialista, comentario, fuente del indicador y estrategia que soporta.

Tabla 37

Indicador Objetivo Estratégico 1

Definición:	Índice de crecimiento de clientes del sector financiero popular y solidario del Nivel 2
Forma de Cálculo:	ICN2=(Nuevos clientes N2/Total de cooperativas N2)*100%
Responsable:	Gerente Comercial
Frecuencia de levantamiento:	Mensual, el 30 de cada mes
Finalidad:	Incrementar los ingresos económicos de la empresa, a partir de la exploración de un nuevo mercado.
Fuente de información:	Sistema de gestión de relacionamiento de clientes, Customer Relationship Management - CRM institucional
Nivel del reporte:	Ejecutivo a la Gerencia General dentro del dashboard
Proceso dentro de la cadena de valor:	Negocios
Especialista:	Gerente de marketing y ventas, Gerente de operaciones, Gerente de Planificación
Comentario:	Para el éxito y logro de la meta planteada por este indicador se debe procurar posicionar sobre la base de la confianza, a la empresa Greenetics como el aliado estratégico de las cooperativas, para el cumplimiento del esquema regulatorio de la SEPS.
Fuente del indicador:	Indicador propuesto por la Alta gerencia como producto de la planificación estratégica, y con la finalidad de cumplir con el objetivo estratégico 1.
Estrategia que soporta:	Lograr el 20 % del mercado de la seguridad de la información en el sector de cooperativas de nivel 2, esto significa que para finales del año 2019 se tendrá 8 clientes nuevos del sector financiero popular y solidario de nivel 2.

Fuente: Greenetics Soluciones S.A.

Elaboración propia

Los indicadores para los objetivos estratégicos, 2 y 3 de encuentran en el anexo 8.

Conclusiones

- La reorientación estratégica de la empresa de servicios de seguridad de la información Greenetics, se basó en la incorporación de una filosofía empresarial de mejora continua, la norma de gestión de la calidad 9001, la norma de seguridad de la información 27001, indicadores de gestión KPI y un código de ética empresarial; todo esto enfocado en alcanzar el mercado del sector financiero de cooperativas de ahorro y crédito del Ecuador.
- Del análisis de estudio de mercado realizado, utilizando fuentes primarias y secundarias, se evidenció lo contenido en la teoría de estrategias especificas respecto de la necesidad de sinergias para lograr oportunidades en mercados grandes o nuevos, por lo que se consideró dentro de la reorientación estratégica la incorporación de actividades tendientes a lograr alianzas estratégicas y acuerdos de cooperación.
- Del análisis realizado a la estructura organizacional de la empresa Greenetics Soluciones S.A. se identificaron debilidades sensibles en su cadena de valor que precisan la adopción de medidas de fortalecimiento sugeridas en la reorientación estratégica, frente a: los desafíos del mercado, las exigencias de las partes interesadas y los riesgos identificados.
- El estado de la seguridad de la información en el sector financiero de cooperativas de ahorro y crédito del Ecuador se encuentra en un proceso de maduración con un 46% de avance, enmarcado principalmente en la regulación y desafíos tecnológicos del sector; se pudo conocer esta realidad gracias al estudio de mercado realizado con una muestra superior al 50% respecto de los activos de los segmentos 1 y 2.
- De la investigación de las filosofías de mejoramiento continuo, para elegir la que mejor se ajusta a una empresa de seguridad de la información, se obtuvo como resultado la empleada por las normativas de la ISO que se sustentan en el círculo virtuoso de Deming. Esto fue corroborado mediante el análisis investigativo hacia otras empresas de similar operación y sirvió de base para la reorientación estratégica.

- Luego del estudio comparativo de los estándares de seguridad de la información, es el estándar ISO 27001 el que mejor se ajusta para apuntalar la reorientación estratégica de la empresa Greenetics, y se considera el más aplicable para este tipo de empresas, por cuanto: maneja la gestión del riesgo, es certificable, tiene amplia aplicabilidad en el país, además de incluir un plan de continuidad del negocio.
- Del estudio de mercado realizado se determinó el grado de influencia que el ecosistema empresarial del sector financiero popular y solidario tiene en una empresa de prestación de servicios de seguridad de la información como Greenetics, para lo cual implementar una metodología de seguridad de la información y un código de ética empresarial resulta obligatorio, tanto por la exigencia del negocio financiero como por su regulación asociada.
- Uno de los principales problemas identificados en el desarrollo de este estudio fue la imposibilidad para Greenetics en abordar empresas grandes y procesos de contratación con montos elevados. La solución planteada es la gestión de nuevas alianzas estratégicas con empresas de mayor poder de negociación y con credenciales adecuadas para participar en procesos de licitación de montos cuantiosos o procesos muy cerrados; de esta forma se pretende lograr participar en los procesos del sector financiero, con montos altos y barreras de entrada, lo cual, además del importante ingreso económico esperado, representa una gran oportunidad de aprendizaje y posibilidad de demostrar las fortalezas de la empresa y de sus profesionales.
- En Greenetics no existe un mecanismo que permita conocer las inquietudes de los clientes respecto de los servicios prestados, por lo que se pierde información valiosa, en el intento de mejorar el nivel y la calidad de los servicios prestados; con la intención de implementar un sistema gestor de la calidad SGC, se observa la necesidad de realizar un levantamiento de datos respecto de los entregables a los clientes, que permita censar la conformidad y canalizar las sugerencias de mejora o necesidades no satisfechas.
- La estructura organizacional de Greenetics Soluciones S.A. está implementada en base a un organigrama funcional, por lo que es necesario que los gerentes entiendan la problemática y procedan a formular su estrategia competitiva que mejor se adapte a la estructura interna de la organización y que interactúe con éxito con el entorno operativo externo, siendo los sistemas de gestión de calidad SGC y de seguridad de la información SGSI los puntales sobre los cuales se estructura la

nueva estrategia competitiva, rescatando una organización funcional con base en procesos.

- El ingreso económico de las cooperativas de ahorro y crédito ha subido en los seis últimos años, no solo por el adecuado manejo financiero que permite el aumento de sus activos, sino también por la minimización de pérdidas económicas, debido al conocimiento del riesgo general y del riesgo operativo, como resultado del impulso a la preparación académica y mejoramiento del nivel cultural de sus profesionales.
- Es entendido por más del 75% de las cooperativas de ahorro y crédito, que un mal manejo del riesgo operativo conlleva cuantiosas pérdidas económicas, motivo por el cual, actualmente la gestión del riesgo operativo es alta en la mayoría de estas organizaciones, quedando claro que en esta era de la digitalización de las finanzas, muy conocida como 'fintech'[8], se considera a los factores tecnológicos y a los ataques informáticos como los más representativos en el riesgo operativo.
- La mayoría de los sistemas de gestión de seguridad de la información y gestión de la calidad, implementados en las cooperativas, no se alinean al giro del negocio, por lo que es una realidad que podría convertirse en un limitante para procesos de inversión en tecnología; bajo esta circunstancia, los temas de seguridad y calidad, se los considera un costo y no una inversión, a excepción de los exigidos por temas regulatorios, que pese a que se los puede también considerar un gasto, se los dota de presupuesto y se los ejecuta para cumplimiento normativo, pero no con el afán de mejorar la operatividad de la institución de economía popular y solidaria.
- La propuesta de estrategia de Greenetics Soluciones S.A. no sólo se ha desarrollado sistemáticamente en base de los recursos y competencias que posee, sino que la nueva estrategia también se fortalece con las normativas impuestas por la industria y su regulación; en este caso específico se han considerado las regulaciones de la Superintendencia de Economía Popular y Solidaria y de la Superintendencia de Bancos, como factor esencial para los nuevos procesos y desarrollo de nuevos servicios y soluciones de seguridad de la información.

[8] 'fintech' es el resultado de la unión de dos palabras en inglés: 'finance' y 'technology', y se refiere a las empresas que nacieron apoyadas en la tecnología para brindar los mismos servicios financieros que otorgan empresas tradicionales, como bancos, compañías de seguros, empresas para envío de remesas, entre otras. Definición obtenida de <www.revistalideres.ec/lideres/ecuador-fintech-tecnologia-desarrollo-banca.html> Consultado en septiembre de 2018.

- Las empresas de seguridad de la información tienen una responsabilidad adicional frente a sus clientes, que consiste en impulsar el desarrollo e implementación de sus sistemas informáticos y de la información, para obtener una ventaja competitiva sostenible; considerando que los beneficios de conocer al cliente y alinearse a sus necesidades del negocio, siempre deben superar las expectativas y niveles de conocimiento, con soluciones innovadoras como nuevas formas de autenticación de los usuarios, que siendo un producto de seguridad de la información y los sistemas, también fortalece sus sistemas informáticos.
- Una vez que Greenetics Soluciones S.A. logre establecer una estrategia exitosa, debe mantenerse ajustando su estrategia a medida que la industria y el entorno evolucionen, por lo que la gerencia ejecutiva encargada finalmente de evaluar el monitoreo y la respuesta del sector financiero popular y solidario, deberá comprender que la mejora continua no se detiene y será la fuente de su éxito, por lo que también deberá verificar e incentivar el desarrollo de sistemas que faciliten el monitoreo continuo de los cambios que ocurren a su alrededor.
- Greenetics Soluciones S.A. debe implementar controles de evaluación del desempeño, basados en indicadores como los tres que se desarrollaron en el presente estudio, que permitan tener reportes de los factores que causan el riesgo operativo a partir de la matriz de riesgo respectiva, para generar planes de acción enfocados en contener, mitigar, minimizar o transferir el riesgo operativo. Estos controles no solo darán una fortaleza operativa, sino también será un factor de intensificación en la generación de confianza hacia los clientes.
- En la planeación, desarrollo, implementación y aplicación de los sistemas gestores de seguridad de la información y de la calidad, es necesario lograr en el entorno más amplio de la empresa Greenetics Soluciones S.A. la participación y apoyo de los dos principales mandantes identificados, estos son la gerencia y la base de trabajadores que aplicarán los sistemas de gestión SGSI y SGC, para lo cual se deberán mejorar los mecanismos y periodicidad de la difusión de los mencionados sistemas, en todas las fases de su implantación.
- El grado de madurez en gestión de la calidad identificado en este estudio, que ha sido logrado por las cooperativas de ahorro y crédito, es sumamente elevado, por lo que se puede esperar una gran aceptación de los proveedores que cumplan con sistemas de gestión de la calidad tales como la ISO 9001; o visto de otra manera, habrá una barrera de entrada muy alta o incluso definitiva para las empresas de

servicios de cualquier naturaleza, más aún para las de servicios de seguridad de la información, que no hayan logrado implementar en sus procesos sustantivos, alguna metodología o filosofía de gestión de la calidad basada en la mejora continua.

- La implementación de las normas ISO 9001 e ISO 27001, conforme a los planes de acción planteados en el presente estudio, permitirán lograr una ventaja competitiva de agregación de valor como socio estratégico hacia el giro del negocio financiero, más que una simple reducción de brecha de las ventajas comparativas, logradas en el sector por otros competidores.
- Implementar normas para mejorar la posición de competitividad de la empresa Greenetics Soluciones S.A. resultará costoso en recursos humanos y económicos, por lo que es muy recomendable implementar normas de similar origen metodológico. En este caso es adecuado para la empresa Greenetics implementar la gestión de la calidad con la ISO 9001 y la gestión de seguridad e la información con la ISO 27001, ya que manejan muchos conceptos y procedimientos simulares, partiendo de orígenes comunes como son la mejora continua y la estructuración soportada en la matriz de riesgos, lo que permite ahorrar recursos y tiempo, tanto en el diseño como en la implementación, e inclusive en la operación a largo plazo.
- La credibilidad y la confianza son valores de suma importancia para las instituciones del sector financiero popular y solidario, por lo que es indispensable que una empresa proveedora de servicios de seguridad de la información, como Greenetics Soluciones S.A., cuente con certificaciones en seguridad de la información y gestión de la calidad, así como un código de ética; factores que le permitirán lograr una aceptación categórica como proveedor de servicios.
- Los planes y acciones enfocados en el mejoramiento del talento humano deberán ayudar a los empleados existentes a adaptarse más rápido al cambio y asegurar que los empleados nuevos lo entiendan de inmediato, manteniendo los recursos dentro de la organización.
- Un hallazgo crítico es el clima laboral, el que se ve degradado por la competencia y rivalidad técnica de los profesionales de Greenetics, lo cual se pretende mejorar con la aplicación de la declaración de ética por parte de cada uno de los empleados de la empresa, lo cual permitirá viabilizar que el modelo propuesto se pueda llevar a la práctica.

- En resumen, dentro de este estudio se ha logrado estructurar una propuesta de reorientación estratégica para la empresa de servicios de seguridad de la información Greenetics Soluciones S.A., incorporando la filosofía de mejora continua tanto en la metodología de calidad total como en la de la seguridad de la información; la implantación de esta propuesta, permitirá lograr la agregación de valor a los procesos fundamentales de la empresa y enfocar los servicios de seguridad de la información hacia el cumplimiento regulatorio vigente para el sector de la economía popular y solidaria, para logar así, dentro de los objetivos estratégicos empresariales, entrar como prestador de servicios en las cooperativas de ahorro y crédito.

Recomendaciones

- Para lograr la reorientación estratégica de la empresa de servicios de seguridad de la información Greenetics se deben aplicar los planes de acción y las tácticas desarrolladas para incorporar la filosofía empresarial de mejora continua, la norma de gestión de la calidad 9001, la norma de seguridad de la información 27001, los indicadores de gestión KPI y el código de ética empresarial.
- Se recomienda que previo a constituir alianzas estratégicas se firme un acuerdo de confidencialidad, Non Disclosure Agreement NDA, para luego validar puntos de acción conjuntos sobre fortalezas complementarias, así como la fórmula de distribución de gastos y utilidades, todo lo cual prontamente deberá ser plasmado en el documento de acuerdo de asociación de alianza estratégica o acuerdo de cooperación.
- Como parte fundamental de la reorientación estratégica se deben aplicar formalmente las medidas de fortalecimiento de la cadena de valor, considerando los desafíos del mercado, las exigencias de las partes interesadas y los riesgos identificados en las matrices de riesgo dadas en el sistema integrado de calidad y seguridad de la información, conforme a las tácticas desarrolladas en el presente trabajo.
- Será de gran utilidad para la aplicación de los planes de acción de la reorientación estratégica, el plasmar en una matriz de cumplimiento regulatorio todas las actividades de seguridad de la información concordantes entre la normativa ecuatoriana y la normativa ISO; lo que permitirá disponer de un documento de trabajo dinámico y específico para el sector financiero de cooperativas de ahorro y crédito del Ecuador, que favorecerá a alinear las actividades empresariales a las expectativas conocidas del estudio de mercado realizado a los segmentos 1 y 2 del sector financiero popular y solidario.
- Para lograr que la filosofía de mejoramiento continuo de las normas ISO se interioricen hacia la cultura organizacional de la empresa Greenetics, es necesaria la formalización de la planificación estratégica desde la alta gerencia, incorporando los controles que aseguren los requerimientos del cliente, los que serán auditados para medir el mejoramiento ganado y finalmente poder tomar las acciones de

corrección, que permita cerrar el círculo virtuoso de Deming de mejoramiento continuo.

- Dentro de la reorientación estratégica de la empresa Greenetics, el estándar ISO 27001 considerado debe estar estructurado sobre una matriz detallada de riesgo, que incluya su mitigación y es necesario proceder a la certificación del proceso principal, que es la consultoría de seguridad de la información.
- Es necesario que el código de ética empresarial sea suscrito por cada empleado que labora en la empresa y que el texto modelo conste publicado para conocimiento de las partes interesadas en la página WEB.
- Es recomendable tener un adecuado protocolo comunicacional antes de iniciar con la implementación del sistema gestor integral de mejora continua, calidad y seguridad de la información, ya que es importante para la supervivencia de la organización y para evitar que este cambio cause desestabilización de la organización actual; por lo tanto es importante gestionar este cambio, hacer del cambio una parametrización al riesgo inherente, con una oportunidad de gestión, para implantar la acción de control que permita gestionar dicho riesgo.
- Para el éxito en la aplicación del SGC y SGSI es necesario considerar la gestión del cambio en perspectiva del talento humano que labora en la empresa, desde la declaración de la misión hasta las pautas de revisión de desempeño, pasando por los programas de orientación para nuevos empleados.

Lista de referencias

Abuhav, Itay. 2017. *ISO 9001:2015: A Complete Guide to Quality Management Systems*. Boca Raton, Florida: Taylor & Francis Group.

"AICPA - American Institute of CPAs". 2018. *AICPA*. Consultado junio 3. https://www.aicpa.org/.

AICPA, ISACA. 2012. *SOC 2 User Guide*. Unite States of America: ISACA. https://www.isaca.org/Groups/Professional-English/isae-3402/Documents/SOC2.pdf.

Antony, Jiju, S Vinodh, y E. V Gijo. 2016. *Lean Six Sigma for Small and Medium Sized Enterprises: A Practical Guide*. https://ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4542933.

BID, OEA. 2016. "Ciberseguridad ¿Estamos preparados en America Latina y el Caribe?" Banco Interamericano de Desarrollo. http://observatoriociberseguridad.org/graph/countries//selected//0/dimensions/1-2-3-4-5.

Brunet, A.P., and New, S. Kaizen in Japan: An Empirical Study. International Journal of Operations and Production Management, Vol. 23(Issue 12), pp. 1426-1446. 2003.

Calder, Alan, y Steve Watkins. 2008. *IT governance: a manager's guide to data security and ISO 27001/ISO 27002*. 4th ed. London ; Philadelphia: Kogan Page Limited.

"cigras2011-cserra-presentacion1 modo de compatibilidad.pdf". 2018. Consultado septiembre 10. https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf.

"Constitución". 2018. Consultado septiembre 29. http://www.seps.gob.ec/documents/20181/25522/CONSTITUCION%20DE%20LA%20REPUBLICA%20DEL%20ECUADOR%20actualizada%20agosto%202018.pdf/d98b1c6a-6d39-4998-8e4d-23372b432883.

Dahlgaard, Jens J, Ghopal K Khanji, y Kai Kristensen. 2007. *Fundamentals of Total Quality Management.* Hoboken: Taylor & Francis. http://public.eblib.com/choice/publicfullrecord.aspx?p=331030.

David, Fred R. 2008. *Conceptos de administración estratégica*. México: Pearson Educación.

Deloitte. 2016. “La evolución de la gestión de ciber-riesgos y seguridad de la información”. Deloitte & Touche S.R.L. https://www2.deloitte.com/pe/es.html.

Dentch, Milton P. 2017. *The ISO 9001:2015 implementation handbook: using the process approach to build a quality management system*. Milwaukee, Wisconsin: ASQ Quality Press.

García-Alcaraz Jorge Luis, Oropesa-Vento Midiala y Maldonado-Macías Aidé Aracely. Kaizen Planning, Implementing and Controlling, Mexico: Springer International Publishing, 2017.

Heras-Saizarbitoria, Iñaki, ed. 2018. *ISO 9001, ISO 14001, and New Management Standards*. Measuring Operations Performance. Cham: Springer.

“Home - Centro de Ciberseguridad Industrial”. 2018. Consultado septiembre 6. https://www.cci-es.org/.

Imai, Masaaki. 2012. *Gemba Kaizen.* Blacklick: McGraw-Hill Publishing. http://public.eblib.com/choice/publicfullrecord.aspx?p=4959285.

Imai, Masaaki. “Gemba Kaizen: A Common-Sense, Low Cost Approach to Management”, New York: McGraw-Hill, 1997.

Imai, Masaaki. Kaizen: The Key to Japan's Competitive Success. New York: Random House, 1986.

INEN. 2016a. “NTE INEN- ISO/IEC TR 27015 Directrices de gestión de seguridad de la información para los servicios financieros”.

———. 2016b. “NTE INEN-ISO 9001 Sistemas de gestión de la calidad — Requisitos”.

———. 2017a. “NTE INEN-ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información – requisitos”.

———. 2017b. “NTE INEN-ISO/IEC 27002:2013 Código de práctica para los controles de seguridad de la información”.

“ISO 9001 Quality management”. 2018. Consultado agosto 11. https://www.iso.org/iso-9001-quality-management.html.

“ISO/IEC 27001 Information security management”. 2018. Consultado junio 8. https://www.iso.org/isoiec-27001-information-security.html.

Kaiser, Abhinav Krishna. 2017. *Become ITIL Foundation certified in 7 days: learning ITIL made simple with real-life examples*. New York: Apress.

"Kaizen Institute Consulting Group". 2018. Consultado agosto 12. https://www.kaizen.com/.

Kesterson, Randy K. 2018. *The Intersection of Change Management and Lean Six Sigma: the basics for black belts and change agents*. Boca Raton: CRC Press, Taylor & Francis Group.

Klosterboer, Larry. 2011. *ITIL capacity management*. 1st ed. Upper Saddle River, NJ: IBM Press/Pearson.

Kumar, Sameer, y Promma Phrommathed. 2005. *New Product Development: An Empirical Study of the Effects of Innovation Strategy, Organization Learning and Market Conditions*. New York, NY: Springer.

"LOEPS". 2018. Consultado septiembre 29. http://www.seps.gob.ec/documents/20181/25522/LEY%20ORGANICA%20DE%20ECONOMIA%20POPULAR%20Y%20SOLIDARIA_reforma_diciembre_2017.pdf/795d5b56-68b9-4eb3-9f86-2ed1edf3f532.

Lareau, William. Office Kaizen Transforming Office Operations into a Strategic Competitive Advantage. Milwaukee: ASQ Quality Press, 2003.

Mika, Geoffrey. Kaizen Event Implementation Manual. Dearborn, Michigan: Society of Manufacturing Engineers, 2006.

"SEPS". 2018. Consultado septiembre 10. https://servicios.seps.gob.ec/gosf-internet/paginas/consultarOrganizaciones.jsf.

"SRI en Línea - Consulta de Impuesto a la Renta y Salida de Divisas". 2018. Consultado septiembre 1. https://declaraciones.sri.gob.ec/sri-en-linea/#/SriDeclaracionesWeb/ConsultaImpuestoRenta/Consultas/consultaImpuestoRenta.

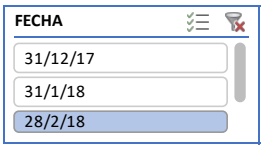
Van Deusen, Cheryl, Steven Williamson, y Harold C Babson. 2007. *Business Policy and Strategy: The Art of Competition, Seventh Edition.* Hoboken: CRC Press. http://public.eblib.com/choice/publicfullrecord.aspx?p=1633548.

Watkins, Steve G. 2008. *An Introduction to Information Security and ISO 27001*. Ely: IT Governance Pub. http://public.eblib.com/choice/publicfullrecord.aspx?p=480419.

Williams, Barry L. 2013. *Information security policy development for compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA standard, PCI DSS V2.0, and AUP V5.0*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Anexos

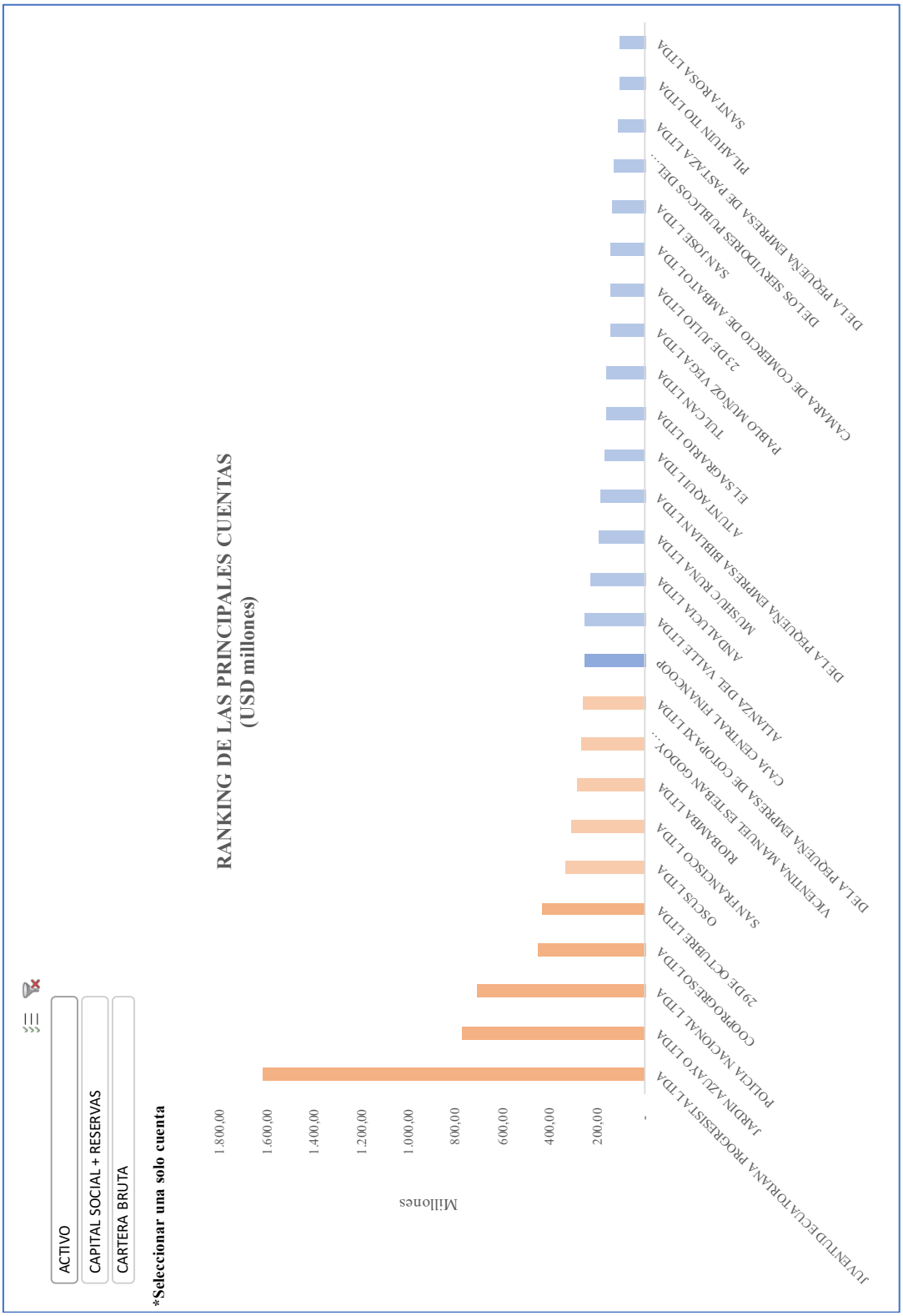
Anexo 1: 64 cooperativas de ahorro y crédito de los segmentos 1 y 2



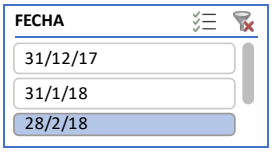
RANKING
SECTOR FINANCIERO POPULAR Y SOLIDARIO SEGMENTO 1
PERIODO DEL 31 DE DICIEMBRE 2017 AL 28 DE FEBRERO 2018
(Dólares)

***Seleccionar una solo fecha**

ENTIDAD	DÓLARES	PROCENTAJE
JUVENTUD ECUATORIANA PROGRESISTA LTDA	1.619.076.950,05	19,86%
JARDIN AZUAYO LTDA	773.953.333,13	9,49%
POLICIA NACIONAL LTDA	711.067.285,69	8,72%
COOPROGRESO LTDA	452.828.397,81	5,55%
29 DE OCTUBRE LTDA	438.385.358,26	5,38%
OSCUS LTDA	338.088.708,88	4,15%
SAN FRANCISCO LTDA	311.596.734,68	3,82%
RIOBAMBA LTDA	286.072.532,49	3,51%
VICENTINA MANUEL ESTEBAN GODOY ORTEGA LTDA	272.188.870,72	3,34%
DE LA PEQUEÑA EMPRESA DE COTOPAXI LTDA	262.363.612,74	3,22%
CAJA CENTRAL FINANCOOP	258.433.228,61	3,17%
ALIANZA DEL VALLE LTDA	254.663.132,56	3,12%
ANDALUCIA LTDA	232.549.034,26	2,85%
MUSHUC RUNA LTDA	198.087.971,47	2,43%
DE LA PEQUEÑA EMPRESA BIBLIAN LTDA	190.774.884,91	2,34%
ATUNTAQUI LTDA	173.723.139,96	2,13%
EL SAGRARIO LTDA	167.462.572,38	2,05%
TULCAN LTDA	165.658.633,90	2,03%
PABLO MUÑOZ VEGA LTDA	147.929.110,98	1,81%
23 DE JULIO LTDA	143.637.589,37	1,76%
CAMARA DE COMERCIO DE AMBATO LTDA	143.305.576,60	1,76%
SAN JOSE LTDA	138.511.532,01	1,70%
DE LOS SERVIDORES PUBLICOS DEL MINISTERIO DE EDUCACIO	134.453.896,59	1,65%
DE LA PEQUEÑA EMPRESA DE PASTAZA LTDA	114.405.826,08	1,40%
PILAHUIN TIO LTDA	112.284.841,91	1,38%
SANTA ROSA LTDA	110.334.657,28	1,35%
Total general	**8.151.837.413,32**	**100,00%**

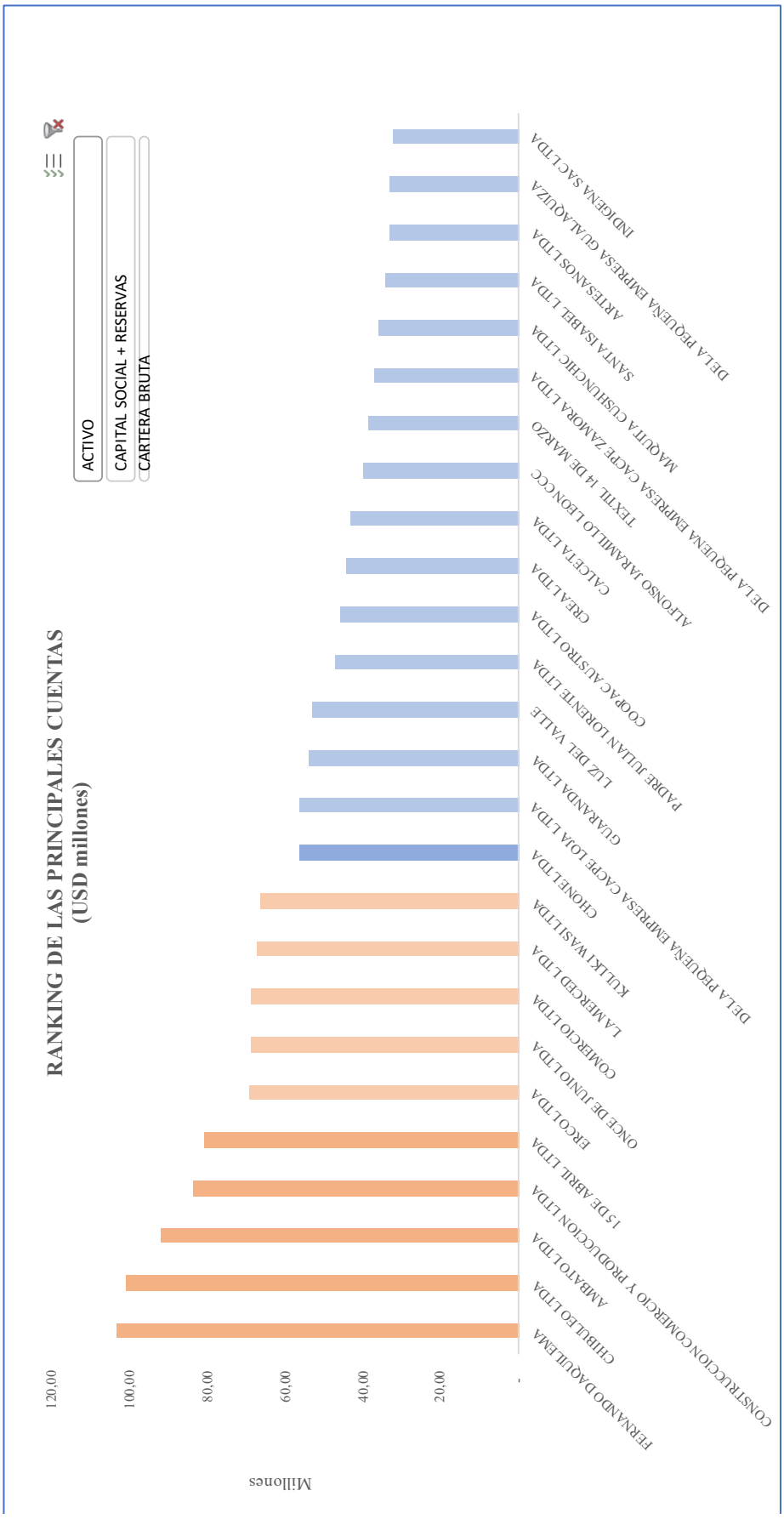

ACTIVO
CAPITAL SOCIAL + RESERVAS
CARTERA BRUTA
*Seleccionar una solo cuenta
RANKING DE LAS PRINCIPALES CUENTAS
(USD millones)
Millones
1.800,00
1.600,00
1.400,00
1.200,00
1.000,00
800,00
600,00
400,00
200,00
-
JUVENTUD ECUATORIANA PROGRESISTA LTDA
JARDIN AZUAYO LTDA
POLICIA NACIONAL LTDA
COOPROGRESO LTDA
29 DE OCTUBRE LTDA
OSCUS LTDA
SANFRANCISCO LTDA
RIOBAMBA LTDA
VICENTINA MANUEL ESTEBAN GODOY...
DELA PEQUEÑA EMPRESA DE COTOPAXI LTDA
CAJA CENTRAL FINANCOOP
ALIANZA DEL VALLE LTDA
ANDALUCIA LTDA
MUSHUC RUNA LTDA
DELA PEQUEÑA EMPRESA BIBLIAN LTDA
ATUNT AQUI LTDA
EL SAGRARIO LTDA
TULCAN LTDA
PABLO MUÑOZ VEGA LTDA
23 DE JULIO LTDA
CAMARA DE COMERCIO DE AMBATO LTDA
DE LOS SERVIDORES PUBLICOS LTDA
SAN JOSE LTDA
DELA PEQUEÑA EMPRESA DE PASTAZA LTDA
PIL AHUIN TIO LTDA
SANTA ROSA LTDA

RANKING
SECTOR FINANCIERO POPULAR Y SOLIDARIO SEGMENTO 2
PERIODO DEL 31 DE DICIEMBRE 2017 AL 28 DE FEBRERO 2018
(Dólares)



***Seleccionar una solo fecha**

ENTIDAD	DÓLARES	PROCENTAJE
FERNANDO DAQUILEMA	103.381.917,73	5,70%
CHIBULEO LTDA	101.199.814,37	5,58%
AMBATO LTDA	92.263.405,51	5,08%
CONSTRUCCION COMERCIO Y PRODUCCION LTDA	83.666.714,39	4,61%
15 DE ABRIL LTDA	81.117.636,56	4,47%
ERCO LTDA	69.182.971,06	3,81%
ONCE DE JUNIO LTDA	69.037.055,93	3,80%
COMERCIO LTDA	68.856.114,53	3,79%
LA MERCED LTDA	67.248.172,98	3,70%
KULLKI WASI LTDA	66.323.769,10	3,65%
CHONE LTDA	56.464.783,23	3,11%
DE LA PEQUEÑA EMPRESA CACPE LOJA LTDA	56.419.924,28	3,11%
GUARANDA LTDA	54.139.045,75	2,98%
LUZ DEL VALLE	53.117.236,23	2,93%
PADRE JULIAN LORENTE LTDA	47.198.176,15	2,60%
COOPAC AUSTRO LTDA	45.929.199,91	2,53%
CREA LTDA	44.484.587,23	2,45%
CALCETA LTDA	43.437.529,56	2,39%
ALFONSO JARAMILLO LEON CCC	40.097.584,08	2,21%
TEXTIL 14 DE MARZO	38.806.625,82	2,14%
DE LA PEQUENA EMPRESA CACPE ZAMORA LTDA	37.037.307,38	2,04%
MAQUITA CUSHUNCHIC LTDA	35.933.413,59	1,98%
SANTA ISABEL LTDA	34.422.037,46	1,90%
ARTESANOS LTDA	33.379.995,74	1,84%
DE LA PEQUEÑA EMPRESA GUALAQUIZA	33.012.558,76	1,82%
INDIGENA SAC LTDA	32.272.184,18	1,78%
SAN ANTONIO LTDA - IMBABURA	31.373.590,33	1,73%
MUJERES UNIDAS TANTANAKUSHKA WARMIKUNAPAC	31.302.253,68	1,72%
JUAN PIO DE MORA LTDA	30.785.095,79	1,70%
VIRGEN DEL CISNE	29.660.719,50	1,63%
PREVISION AHORRO Y DESAROLLO LTDA	28.489.164,10	1,57%
COTOCOLLAO LTDA	28.234.850,68	1,56%
ARMADA NACIONAL	26.706.414,33	1,47%
EDUCADORES DEL AZUAY LTDA	26.463.174,46	1,46%
LUCHA CAMPESINA	25.887.568,04	1,43%
EDUCADORES DE LOJA LTDA	24.549.283,60	1,35%
SAN FRANCISCO DE ASIS LTDA	21.607.467,31	1,19%
MAS AHORRO SOLIDARIO MASCOOP	21.584.569,68	1,19%
Total general	**1.815.073.913,01**	**100,00%**


RANKING DE LAS PRINCIPALES CUENTAS
(USD millones)
ACTIVO
CAPITAL SOCIAL + RESERVAS
CARTERA BRUTA
Millones
120,00
100,00
80,00
60,00
40,00
20,00
-
FERNANDO DAQUILEMA
CHIBULEO LTDA
AMBATO LTDA
CONSTRUCCION COMERCIO Y PRODUCCION LTDA
15 DE ABRIL LTDA
ERCO LTDA
ONCE DE JUNIO LTDA
COMERCIO LTDA
LA MERCED LTDA
KULKI WASI LTDA
CHONE LTDA
DE LA PEQUEÑA EMPRESA CACPE LOJA LTDA
GUARANDA LTDA
LUZ DEL VALLE
PADRE JULIAN LORENTE LTDA
COOP AC AUSTRO LTDA
CREA LTDA
CALCETA LTDA
ALFONSO JARAMILLO LEON CC
TEXTIL 14 DE MARZO
DE LA PEQUEÑA EMPRESA CACPE ZAMORA LTDA
MAQUITA CUSHUNCHIC LTDA
SANTA ISABEL LTDA
ARTESANOS LTDA
DE LA PEQUEÑA EMPRESA GUALAQUIZA
INDIGENA SAC LTDA

Anexo 2: Asociaciones de Cooperativas de Ahorro y Crédito

Para la entrevista se ha considerado un sector representativo de las Cooperativas de Ahorro y Crédito, las 6 asociaciones que actualmente tienen estructura y representación, y cuentan con el apoyo de sus agremiados

1) ICORED:

Nombre:	Red de Integración Ecuatoriana de Cooperativas de Ahorro y Crédito
Dirección:	Inglaterra E3-263 y Av. Amazonas Edificio Centro Ejecutivo, Piso 7, Oficina 701, Quito
Teléfono:	(593-2)2272827 / 2457700
Presidente:	Ing. Estuardo Paredes - Gerente COAC San Francisco

2) RFD:

Nombre:	Red de Instituciones Financieras de Desarrollo
Dirección:	Pasaje El Jardín E10-06 y Av. 6 de Diciembre Edif. Century Plaza. Piso 8, Quito
Teléfono:	(593-2) 333-2446 / 333-2446 / 333-3091 / 333-3091
Presidente:	Econ. Fausto Jordán -

3) UCACSUR:

Nombre:	Unión de Cooperativas de Ahorro y Crédito del SUR
Dirección:	Padre Aguirre 15-24 y Rafael María Arízaga Edificio Bellavista - Cuenca
Teléfono:	(07) 2 838195
Presidente:	Juan Pablo Guerra

4) UCACNOR:

Nombre:	Unión de Cooperativas de Ahorro y Crédito del Norte
Dirección:	José Joaquín Olmedo & Luis Fernando Villamar, Ibarra
Teléfono:	Fijo: 06 2611 389 / 06 2611 809 - Ext. 101 Móvil: 0987380231

Presidente:	Ing. César Cifuentes

5) UCACCENTRO:

Nombre:	Unión De Cooperativas De Ahorro Y Crédito Del Centro
Dirección:	Pacha 07-85 y Paltas 180104 Ambato
Teléfono:	(03) 240-1721
Presidente:	El Ing. Rodrigo Llambo -

6) FECOAC:

Nombre:	Federación Nacional de Cooperativas de Ahorro y Crédito
Dirección:	Quito, AV. Colon y Diego de Almagro Edifico El cisne Piso 3
Teléfono:	(593) 22222-786
Presidente:	Milton Barreiro

Anexo 3: Encuesta de riesgo en cooperativas

Encuesta Riesgo en Cooperativas

I. RIESGO

Pregunta 1. ¿Su conocimiento sobre riesgos es?

Opción	Bajo	Medio	Alto	Muy Alto	Completo
Respuesta			X		

Pregunta 2. ¿Tiene alguna capacitación en riesgos?

Opción	Si	No
Respuesta		X

Pregunta 3. ¿Existe la cultura de riesgo en su cooperativa?

Opción	Si	No	No sabe
Respuesta	X		

Pregunta 4. ¿Su conocimiento sobre riesgo operativo es?

Opción	Bajo	Medio	Alto	Muy Alto	Completo
Respuesta			X		

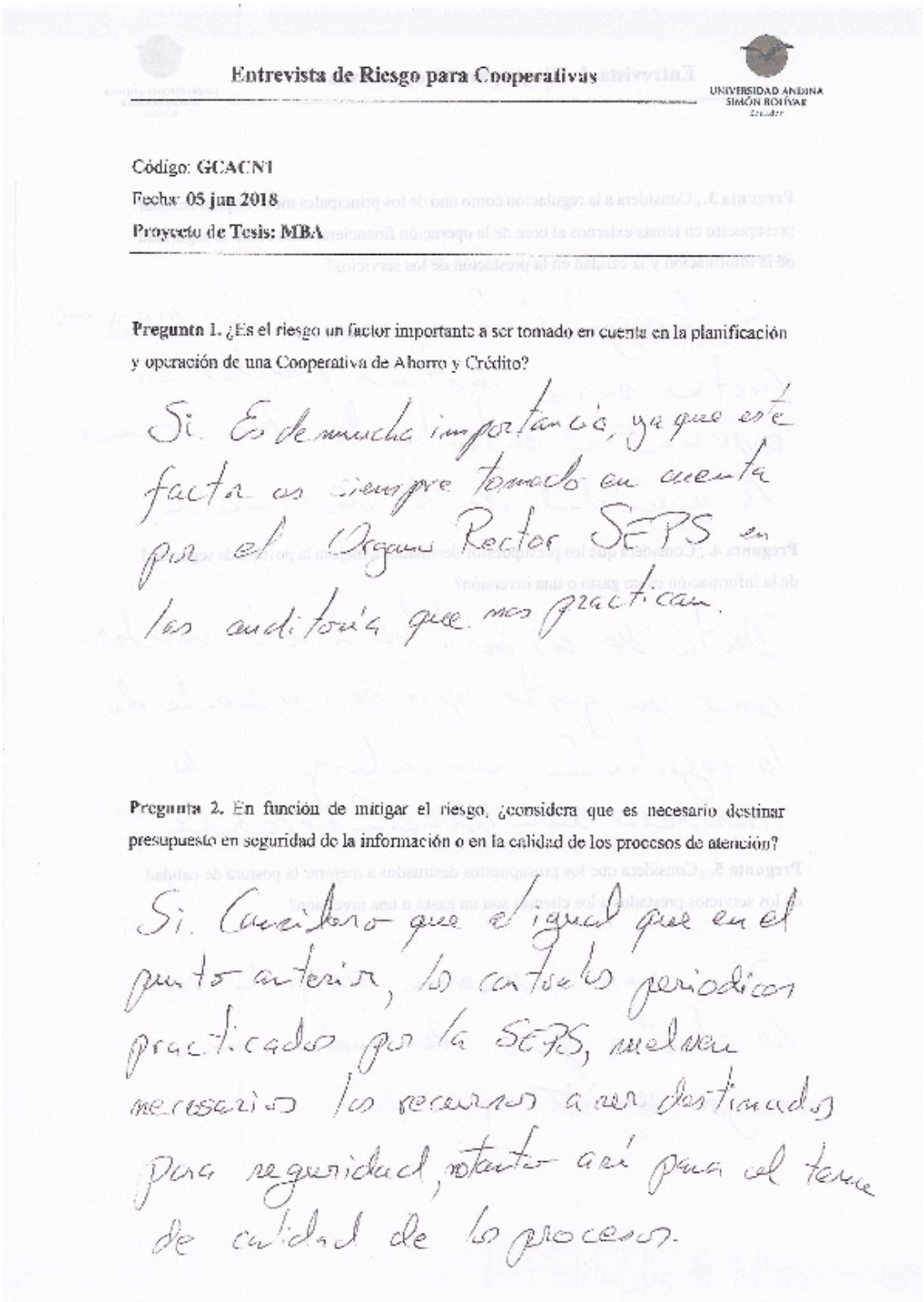
Pregunta 5. ¿Se gestiona el riesgo operativo en su cooperativa?

Opción	Si	No	No sabe
Respuesta	X		

Pregunta 6. ¿Qué factores influyen sobre el riesgo operativo? Del 1 al 5, considerando que 5 es el que mas influye y 1 el que menos influye

Opción	Procedimientos	Empleados	Tecnología	Clientes	Ataques informáticos
Respuesta	1	2	5	4	3

Anexo 4: Entrevista de riesgo para cooperativas de ahorro y crédito



Entrevista de Riesgo para Cooperativas

UNIVERSIDAD ANDINA SIMÓN BOLÍVAR
Ecuador

Código: GCACN1
Fecha: 05 jun 2018
Proyecto de Tesis: MBA

Pregunta 1. ¿Es el riesgo un factor importante a ser tomado en cuenta en la planificación y operación de una Cooperativa de Ahorro y Crédito?

Si. Es de mucha importancia, ya que este factor es siempre tomado en cuenta por el Organo Rector SEPS en las auditorías que nos practican.

Pregunta 2. En función de mitigar el riesgo, ¿considera que es necesario destinar presupuesto en seguridad de la información o en la calidad de los procesos de atención?

Si. Considero que el igual que en el punto anterior, los controles periodicos practicados por la SEPS, mediran necesario los recursos a ser destinados para seguridad, notando así para el tema de calidad de los procesos.

Anexo 5: Matriz FODA

		FORTALEZAS		DEBILIDADES	
		F1	Personal con adecuada capacitación	D1	Falta de comunicación
		F2	Profesionales con aptitud	D2	Retardo en presentación de ofertas comerciales
		F3	Experiencia en seguridad de la información	D3	Plan estratégico
		F4	Cumplimiento de los SLA	D4	Seguimiento de actividades
		F5	Satisfacción de los clientes en los servicios entregados	D5	Falta de detalle en el material de capacitación
		F6	Poca burocracia interna	D6	Falta de dirección
		F7	Costo de los servicios	D7	Red de contactos de alto nivel
		F8	Red de contactos profesionales	D8	Reducida cantidad de clientes en el sector financiero
		F9	Alianzas estratégicas	D9	Fuerza de ventas
		F10	Reputación de la empresa	D10	Garantías financieras
		F11	Actitud a enfrentar nuevos retos	D11	Solo tiene operación en Quito
		F12	Capacidad y experiencia en curso y talleres	D12	Indicadores financieros
				D13	flujo de efectivo
				D14	Precio de los servicios
OPORTUNIDADES	O1	El mercado financiero popular y solidario no esta muy explotado aun			
	O2	Existe regulación que exige seguridad de la información		(D1, D2, D3, D4, D5, O1, O2, O3, O4, O6) Obtener una certificación en Seguridad de la información	
	O3	Incremento y conciencia frente a los ataques informáticos	(F1, F2, F3, F4, F5, F7, F8, F10, O4, O5, O6)Ofrecer servicios preventivos de seguridad en modalidad de outsoursing	(D1, D2, D3, D4, D5, D8, D14, O1, O2) Obtener una certificación de Gestión de la Calidad	
	O4	Aumento de los riesgos de los activo en las cooperativas por ataques informáticos	(O1, O2, O3, F3, F10, F11) Diseñar un servicio de consultoría enfocado en mejorar la posición de seguridad de las Cooperativas y facilitar un cumplimiento práctico de la normativa SEPS	(O1, O2, O3, D11, D7, D8) Generar alianzas estratégicas en otras ciudades del Ecuador enfocadas en prestas servicios y capacitaciones locales, a cooperativas fuera del entorno capitalino.	
	O5	Bajo conocimiento de medidas de seguridad internas de las cooperativas	(O3, O4, O5, O6, F1, F2, F3, F11, F12) Ofrecer un servicio de capacitación especializada de seguridad a las cooperativas, con talleres prácticos lineados a cumplir normativa nacional SEPS y certificaciones internacionales ISO 27015 o PSI	(O1, O2, O3, D7, D8, D10, D12, D13) Generar y fortalecer alianzas estratégicas en enfocadas en prestar servicios en contratos grandes a cooperativas, bancos e instituciones financieras del estado.	
	O6	Preocupación por vulnerabilidades en activos y aplicativos		(D9, D11, D7, D2, O1, O2, O3) Aumentar la fuerza de ventas tanto de nómina, como por comisionamiento	
AMENAZAS	A1	Legislación débil			
	A2	Autoridad controladora no tan exigente			
	A3	Incremento del número de empresas de seguridad de la información	(A3, A4, A6, A7, F10, F5, F3, F2) Iniciar una campaña márquetin diferenciadora de la competencia	(D9, D7, D8, A3, A4, A6, A7) Entregar cursos promocionales a los potenciales clientes .	
	A4	Presupuestos no consideran seguridad por problemas macroeconómicos	(F6, F7, F9, A3, A5, A7) Manejar una estrategia de precios para no perder clientes que no tienen presupuesto o que solo contratan por precio	(O1, O2, O3, O4, D13, D11, D7)Investigar la posibilidad de ingresar a mercados extranjeros	
	A5	Austeridad de gasto publico para inversiones	(F1, F2, F3, F4, F9, F10, A3, A5, A6, A7) Ofrecer y realizar pruebas de concepto	(D8, D9, A1, A2, A3, A4) Analizar la posibilidad de sacar otra línea de negocios como puede ser la de reciclaje de computadores	
	A6	Exceso de confianza por parte de los administradores de seguridad			
	A7	Dificultad de vender productos para una empresa nueva			

Anexo 6: Código de ética

OFICIAL DE SEGURIDAD DE GREENETICS
CODIGO DE ETICA

Como oficial de seguridad de la información de Greenetics Soluciones S.A., me considero miembro de una organización importante y honorable.

Reconoceré la relación positiva entre un buen acondicionamiento físico y mental y el desempeño de mi trabajo.

Realizaré mi deber con eficiencia lo mejor que pueda.

Mi conducta y el desempeño de mis funciones se realizarán de manera honesta, contribuyendo a mis compañeros de trabajo y observando las leyes de la ciudad, el estado y el país.

En el desempeño de mi deber no trabajaré para obtener una ventaja o beneficio no ético.

Reconoceré en todo momento en mi deber que soy un empleado de seguridad, y que en última instancia soy responsable ante los clientes y la comunidad.

Daré el servicio más eficiente e imparcial del que soy capaz en todo momento.

Entiendo la importancia de la cortesía y la mantendré como mi punto de referencia en todos mis deberes.

Consideraré a mis colegas con los mismos estándares que me mantengo.

Comparto una afinidad recíproca y una obligación con mis compañeros de trabajo, mi organización y mis clientes.

Aceptaré la responsabilidad de mis acciones.

Buscaré esos valores que reflejarán honor en mis colegas de Greenetics, mis clientes y yo mismo.

_____ ***Yo juro cumplir con lo anterior.***

_____ ***Yo me reafirmo en lo anterior.***

_____ *Fecha* _____
Firma

_____
Nombre

Anexo 7: tácticas y planes de acción para las estrategias 3, 4, 5, 6, 7, 8 y 9

3) Generar alianzas estratégicas en otras ciudades del Ecuador enfocadas en prestar servicios y capacitaciones locales, a cooperativas fuera del entorno capitalino.

Táctica o Plan de Acción 1: Preparación empresarial operativa

- E3T1.1: Firmar el código de ética y ponerlo a conocimiento de las partes interesadas, de manera general.
- E3T1.2: Revisar Políticas de relación con otras empresas, tanto administrativas como operacionales.
- E3T1.3: Revisar procedimientos de compartición de información, modelos de acuerdos de confidencialidad NDA, modelos de acuerdos comerciales y alianzas estratégicas.

Táctica o Plan de Acción 2: Preparación empresarial económica

- E3T2.1: Revisar costos y márgenes de utilidad de la propuesta económica para la participación en una alianza estratégica o acuerdo comercial, dependiendo del tipo de servicio o producto que se pretende comercializar conjuntamente, costos por cambio de plaza y movilización.
- E3T2.2: Revisar costos y márgenes de la cartera de servicios y productos que se pretende comercializar conjuntamente, y los costos de servicios profesionales.

Táctica o Plan de Acción 3: Preparación relación empresarial

- E3T3.1: Participación en redes sociales, principalmente LinkeIn y para el tema de capacitación Facebook.
- E3T3.2: Evaluar potenciales aliados estratégicos de la misma cartera de profesionales capacitados en la academia.
- E3T3.3: Evaluar las potenciales alianzas estratégicas respecto del valor agregado conjunto que se puede lograr, el aumento de captación de mercado posible, la transferencia tecnológica que se puede lograr, el probable aumento de oportunidades de negocios por una mayor presencia a nivel nacional.

4) Generar y fortalecer alianzas estratégicas enfocadas en prestar servicios en contratos grandes a cooperativas, bancos e instituciones financieras del estado.

Táctica o Plan de Acción 1: Preparación empresarial operativa

- E4T1.1: Obtener las Normas ISO 9001 27001:2018 y poner la política integrada en un repositorio que pueda ser compartido y accedido por todas las partes interesadas.
- E4T1.2: Revisar Políticas de relación con otras empresas, tanto administrativas como operacionales.
- E4T1.3: Revisar procedimientos de compartición de información, modelos de acuerdos de confidencialidad NDA, modelos de acuerdos de alianza estratégica.

Táctica o Plan de Acción 2: Preparación empresarial económica

- E4T2.1: Revisar costos y márgenes de utilidad de la propuesta económica para la participación en una alianza estratégica, dependiendo del tipo de servicio o producto que se pretende comercializar conjuntamente.
- E4T2.2: Revisar costos y márgenes de la cartera de servicios y productos que se pretende comercializar conjuntamente.

Táctica o Plan de Acción 3: Preparación relación empresarial

- E4T3.1: Participación en eventos nacionales tales como Ciberseguridad en Banca y Gobierno, eventos que organizan las asociaciones de cooperativas de ahorro y crédito, eventos que organiza la Superintendencia de Economía Popular y Solidaria - SEPS.
- E4T3.2: Participar en eventos internacionales, como ISACA, FELABAN y de fabricantes de los productos.
- E4T3.3: Evaluar las alianzas estratégicas y validar nuevas posibilidades de alianzas, considerando el valor agregado conjunto que se puede lograr, el aumento de captación de mercado posible, la transferencia tecnológica que se puede lograr, el probable aumento de oportunidades de negocios.

5) Aumentar la fuerza de ventas tanto de nómina, como por comisionamiento, con el propósito de visitar cooperativas de ahorro.

Táctica o Plan de Acción 1: Preparación empresarial operativa

- E5T1.1: Estructurar y aplicar el uso de un Sistema gestor de relacionamiento con el cliente, por siglas en Inglés CRM - Customer relationship management, para toda el área comercial.
- E5T1.2: Reestructurar el área comercial conforme a las consideraciones de calidad y mejora continua de la ISO 9001.

Táctica o Plan de Acción 2: Preparación Recurso Humano

- E5T2.1: Certificar a los profesionales que serán encargados de la implementación y uso del sistema de gestión de relación con clientes CRM.
- E5T2.2: Realizar una capacitación interna de gestión de ventas, respecto de los productos propios y ofrecidos en alianza estratégica.
- E5T2.3: Realizar un coaching para motivar al personal y alinearlo al nuevo reto de la empresa, tendiente a lograr la adopción de un funcionamiento con CRM.
- E5T2.4: Fortalecimiento de la fuerza de ventas, mediante el reclutamiento de profesionales de ventas por comisión de ventas.

6) Iniciar una campaña diferenciadora de mercadeo digital, a fin de posicionar a la empresa como un referente de la seguridad de la información en cooperativas;

Táctica o Plan de Acción 1: Preparación empresarial operativa

- E6T1.1: Estructurar un plan digital de mercadeo, enfocado en redes sociales y asociado al CRM para obtención de oportunidades de negocio.
- E6T1.2: Reestructurar el área comercial conforme a las consideraciones de calidad y mejora continua de la ISO 9001, para incorporar funcionalidades de mercadeo digital.

Táctica o Plan de Acción 2: Preparación Recurso Humano

- E6T2.1: Certificar a los profesionales que serán encargados de la implementación y uso del sistema de gestión de relación con clientes CRM.
- E6T2.2: Realizar una capacitación interna de gestión de mercadeo, respecto de los productos propios y ofrecidos en alianza estratégica.
- E6T2.3: Realizar eventos propios y correlacionados con los cursos de capacitación para sintetizar las oportunidades de negocios en los nuevos mercados como el del sector financiero popular y solidario.

7) Manejar una estrategia de precios para no perder cooperativas de ahorro y crédito que no tienen presupuesto o que sólo contratan por precio y para cumplir con la regulación de la SEPS;

Táctica o Plan de Acción 1: Reducción de costos operativos

- E7T1.1: Sobre la base del nuevo esquema de procesos, determinar la reducción de costos operativos, en base a la eficiencia por la aplicación de la norma ISO 9001, que conlleva optimización de recursos, automatización de tareas repetibles, minimización de gastos.
- E7T1.2: Mejora del uso de recursos compartidos, economía de escala para la prestación de servicios y soluciones de seguridad de la información.

Táctica o Plan de Acción 2: Nuevos servicios respecto de la normativa

- E7T2.1: Estructurar nuevos servicios de seguridad de la información sobre la base de las nuevas normativas, con opciones de bajo costo y economías de escala.

8) Diseñar un servicio de consultoría enfocado en mejorar la posición de seguridad de las Cooperativas y facilitar un cumplimiento práctico de la normativa SEPS.

Táctica o Plan de Acción 1: Revisión de la normativa

- E8T1.1: Sobre la base del nuevo esquema regulatorio emitido por la Superintendencia de Economía Popular y Solidaria, desarrollar una matriz de requerimientos que puedan ser agrupados en un producto de consultoría y asesoramiento para su cumplimiento.

Táctica o Plan de Acción 2: Revisión de productos

- E8T2.1: Validar con que productos de seguridad se puede satisfacer las necesidades de cumplimento regulatorio exigida por la SEPS.

Táctica o Plan de Acción 3: Desarrollo del producto de consultoría

- E8T3.1: Diseñar la arquitectura de un nuevo servicio de consultoría enfocado en el cumplimiento de la matriz de exigencia de seguridad de la información para cumplimiento regulatorio.

- E8T3.2: Elaborar el material del producto de consultoría de seguridad SEPS, tales como presentaciones, material de apoyo, talleres de concientización y curso de preparación.

9) Ofrecer un servicio de capacitación especializada de seguridad a las cooperativas, con talleres prácticos lineados a cumplir normativa nacional SEPS y certificaciones internacionales ISO 27015 o PSI.

Táctica o Plan de Acción 1: Revisión de la normativa

- E9T1.1: Sobre la base del nuevo esquema regulatorio emitido por la Superintendencia de Economía Popular y Solidaria, desarrollar una matriz de requerimientos que puedan ser agrupados en un producto de capacitación especializada en cumplimento de normativa.
- E9T1.2: Parametrizar a la matriz de requerimientos de seguridad de la información de la SEPS, los temas de interés respecto de la ISO 27015 y PCI DCS, que puedan ser agrupados en un producto de capacitación especializada en cumplimento de normativa.

Táctica o Plan de Acción 2: Revisión de capacitadores

- E9T2.1: Validar con que profesionales de seguridad se puede iniciar una nueva propuesta de curso, destinado satisfacer las necesidades de cumplimento regulatorio exigida por la SEPS, y con conocimientos en ISO 27015 y PCI DCS.

Táctica o Plan de Acción 3: Desarrollo del curso de capacitación

- E9T3.1: Diseñar la malla y syllabus de un nuevo curso - taller enfocado en el cumplimiento de la matriz de exigencia de seguridad de la información para cumplimiento regulatorio de la SEPS
- E9T3.2: Elaborar el material del curso de seguridad de la información SEPS, tales como presentaciones, material de apoyo, talleres prácticos y documentos de aprobación del curso.

Anexo 8: Indicadores objetivos estratégicos 2 y 3

Indicador Objetivo Estratégico 2

Definición:	Índice de crecimiento de clientes del sector financiero popular y solidario del Nivel 1
Forma de Cálculo:	ICN1=(Nuevos clientes N1/Total de cooperativas N1)*100%
Responsable:	Gerente Comercial
Frecuencia de levantamiento:	Mensual, el 30 de cada mes
Finalidad:	Incrementar los ingresos económicos de la empresa, a partir de la exploración de un nuevo mercado, soportado en las alianzas estratégicas necesarias para llegar al sector financiero popular y solidario N1
Fuente de información:	Sistema de gestión de relacionamiento de clientes, Customer Relationship Management - CRM institucional; así como la base de clientes prospectados conjuntamente en alianza estratégica.
Nivel del reporte:	Ejecutivo a la Gerencia General dentro del dashboard
Proceso dentro de la cadena de valor:	Negocios
Especialista:	Gerente de marketing y ventas, Gerente de operaciones, Gerente de Planificación
Comentario:	Para el éxito y logro de la meta planteada por este indicador se debe procurar posicionar sobre la base de la confianza, a la empresa Greenetics como el aliado estratégico de las cooperativas, para el cumplimiento del esquema regulatorio de la SEPS. Con el apoyo de la empresa que apoyará en la prestación de los nuevos servicios.
Fuente del indicador:	Indicador propuesto por la Alta gerencia como producto de la planificación estratégica, y con la finalidad de cumplir con el objetivo estratégico 2.

Estrategia que soporta:	Lograr el 12% de mercado de la seguridad de la información en el sector de cooperativas de nivel 1, esto significa que para finales del año 2019 se tendrán 3 clientes nuevos del sector financiero popular y solidario de nivel 1.

Fuente: Greenetics Soluciones S.A.

Elaboración propia

Indicador Objetivo Estratégico 3

Definición:	Índice de crecimiento de ventas por aumento de cursos para los clientes del sector financiero popular y solidario
Forma de Cálculo:	ICV=(Venta de cursos cumplimiento SEPS/Total de venta de cursos)*100%
Responsable:	Gerente Comercial
Frecuencia de levantamiento:	Mensual, el 30 de cada mes
Finalidad:	Incrementar los ingresos económicos de la empresa, a partir de la exploración de un nuevo mercado.
Fuente de información:	Sistema de gestión de relacionamiento de clientes, Customer Relationship Management - CRM institucional
Nivel del reporte:	Ejecutivo a la Gerencia General dentro del dashboard
Proceso dentro de la cadena de valor:	Negocios
Especialista:	Gerente de marketing y ventas, Gerente de operaciones, Gerente de Planificación
Comentario:	Para el éxito y logro de la meta planteada por este indicador se debe procurar posicionar sobre la base de la confianza, a la empresa Greenetics como referente en el tema de capacitación hacia las cooperativas, para el cumplimiento del esquema regulatorio de la SEPS.
Fuente del indicador:	Indicador propuesto por la Alta gerencia como producto de la planificación estratégica, y con la finalidad de cumplir con el objetivo estratégico 3.
Estrategia que soporta:	Lograr un aumento de los ingresos por cursos en un 10%, con la incorporación de al menos un taller teórico - práctico diseñado para que las cooperativas de ahorro y crédito logren su cumplimiento regulatorio, con énfasis en seguridad de la información, riesgos operativos, plan de continuidad del negocio y cumplimiento de la regulación de la SEPS.

Fuente: Greenetics Soluciones S.A.

Elaboración propia

Anexo 9: Normativa vigente sobre seguridad de la información para instituciones financieras y cooperativas

1. Control de seguridades en el uso de transferencias electrónicas SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 y su reforma SEPS-IGT-IR-ISF-ITIC-IGJ-2017-113.
2. Norma de Control para la seguridad física y electrónica SEPS-IGT-IR-IGJ-2018-021.
3. Norma de control para el envío y recepción información y notificaciones SEPS-IGT-IR-IGJ-2018-016.
4. Para gestión de riesgo operativo Resolución JB-2014-3066

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103

KLÉVER MEJÍA CAGUASANGO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (E)

CONSIDERANDO:

Que, el Código Orgánico Monetario y Financiero publicado en el Segundo Suplemento del Registro Oficial No. 332 de 12 de septiembre de 2014, regula los sistemas monetarios y financieros, así como los regímenes de valores y seguros del Ecuador;

Que, el numeral 1 del artículo 62, en concordancia con el inciso segundo del artículo 74 del mencionado Código determina como función de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión de las disposiciones del Código Orgánico Monetario y Financiero;

Que, el numeral 7 del artículo 62 del aludido Código, establece como función de la Superintendencia de Economía Popular y Solidaria, velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente, preventiva, extra situ y visitas de inspección in situ que permitan determinar la situación económica y financiera de las entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan;

Que, el último inciso del artículo 62 ibídem determina que la Superintendencia de Economía Popular y Solidaria para el cumplimiento de sus funciones, podrá expedir las normas en las materias propias de su competencia sin que pueda alterar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Monetaria y Financiera;

Que, el inciso primero del artículo 74 del citado cuerpo legal, dispone que la Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se regirán por las disposiciones de dicho Código y la Ley Orgánica de Economía Popular y Solidaria;

Que, en el artículo 163 del referido Código, determina que las cooperativas de ahorro y crédito, las cajas centrales y las asociaciones mutualistas de ahorro y crédito para la vivienda forman parte del sector financiero popular y solidario;

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-113

KLÉVER MEJÍA CAGUASANGO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (S)

CONSIDERANDO:

Que, mediante resolución No SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 de 23 de noviembre de 2017, la Superintendencia de Economía Popular y Solidaria expidió la "NORMA DE CONTROL DE LAS SEGURIDADES EN EL USO DE TRANSFERENCIAS ELECTRÓNICAS", que deben aplicar las cooperativas de ahorro y crédito, las cajas centrales y las asociaciones mutualistas de ahorro y crédito para la vivienda;

Que, el inciso segundo del artículo 73 del Código Orgánico Monetario y Financiero, en concordancia con el último inciso del artículo 74 de dicho cuerpo legal, respecto de la Superintendencia de Economía Popular y Solidaria, determina que: *"Los actos normativos podrán ser reformados o derogados en cualquier tiempo, por parte del órgano que lo expidió o a petición de parte, mediante la presentación de un reclamo administrativo."*;

Que, es necesario facilitar el acceso a herramientas tecnológicas que estén disponibles para el sector financiero popular y solidario; y,

Que, mediante acción de personal No. 1910 de 20 de diciembre de 2017, se dispone la subrogación de Superintendente de Economía Popular y Solidaria, en favor de Kléver Mejía Caguasango;

En ejercicio de las atribuciones y las funciones que le confiere la Ley, resuelve expedir la siguiente:

REFORMA A LA RESOLUCIÓN No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 DE 23 DE NOVIEMBRE DE 2017

Artículo Único.- Sustitúyase el numeral 2 del artículo 4, de la Sección III, por el siguiente:

"2.- Contar con privilegios de autorización y medidas de autenticación, controles de acceso lógicos que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que es". Las entidades podrán implementar otros mecanismos de seguridad con el fin de precautelar la transacción"

DISPOSICIÓN FINAL.- La presente resolución entrará en vigencia a partir de la presente fecha, sin perjuicio de su publicación en el Registro Oficial.

Publíquese en la página web de la Superintendencia de Economía Popular y Solidaria.

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN No. SEPS-IGT-IR-IGJ-2018-021

CATALINA PAZOS CHIMBO

SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (E)

CONSIDERANDO:

Que, el Código Orgánico Monetario y Financiero publicado en el Segundo Suplemento del Registro Oficial No. 332 de 12 de septiembre de 2014, regula los sistemas monetarios y financieros, así como los regímenes de valores y seguros del Ecuador;

Que, el numeral 1 del artículo 62, en concordancia con el inciso segundo del artículo 74 del mencionado Código determina como función de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión de las disposiciones del Código Orgánico Monetario y Financiero y de las regulaciones dictadas por la Junta de Política y Regulación Monetaria y Financiera, en lo que corresponda a las actividades financieras ejercidas por las entidades que conforman el sector financiero popular y solidario;

Que, el numeral 7 del artículo 62 del aludido Código, establece como función de la Superintendencia de Economía Popular y Solidaria, velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente preventiva extra situ y visitas de inspección in situ, que permitan determinar la situación económica y financiera de las entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan;

Que, el último inciso del artículo 62 ibídem determina que la Superintendencia de Economía Popular y Solidaria para el cumplimiento de sus funciones, podrá expedir las normas en las materias propias de su competencia sin que pueda alterar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Monetaria y Financiera;

Que, el inciso primero del artículo 74 del citado cuerpo legal, dispone que la Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se regirán por las disposiciones de dicho Código y la Ley Orgánica de la Economía Popular y Solidaria;

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN N° SEPS-IGT-SGE-IGJ-2018- 016

CATALINA PAZOS CHIMBO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA (E)

CONSIDERANDO

Que el artículo 146 inciso primero de la Ley Orgánica de Economía Popular y Solidaria prescribe: "*El control de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario estará a cargo de la Superintendencia de Economía Popular y Solidaria, que se crea como organismo técnico, con jurisdicción nacional, personalidad jurídica de derecho público, patrimonio propio y autonomía administrativa y financiera y con jurisdicción coactiva.*";

Que el artículo 12 de dicho cuerpo legal determina: "*Para ejercer el control y con fines estadísticos las personas y organizaciones registradas presentarán a la Superintendencia, información periódica relacionada con la situación económica y de gestión, de acuerdo con lo que disponga el Reglamento de la presente Ley y cualquier otra información inherente al uso de los beneficios otorgados por el Estado.*";

Que el artículo 167 literal e) de la referida ley orgánica establece como una de las obligaciones de las organizaciones por ella amparadas: "*Dar todas las facilidades para que los órganos de control y regulación cumplan sus funciones;*";

Que de conformidad con el artículo 74 del Código Orgánico Monetario y Financiero, la Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se rige por las disposiciones del Código y la Ley de Economía Popular y Solidaria;

Que los incisos primero y segundo del artículo 242 del mencionado Código Orgánico prescriben: "*Las entidades del sistema financiero nacional están obligadas a entregar la información que les sea requerida por los organismos de control y el Servicio de Rentas Internas, de manera directa, sin restricción, trámite o intermediación alguna, en las condiciones y forma que estas entidades lo dispongan, exclusivamente para fines de su gestión.*

La información legal, financiera, contable y de cualquier otro tipo que sea requerida a las entidades sujetas a este Código por los respectivos organismos de control podrá ser desmaterializada y suscrita por medio de firma electrónica debidamente certificada por una de las entidades autorizadas, en los términos previstos en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Cada organismo de control establecerá, para su implementación, las disposiciones inherentes a cada tipo de información.";

Junta Bancaria del Ecuador

RESOLUCIÓN JB-2014-3066

LA JUNTA BANCARIA

CONSIDERANDO:

Que en titulo X "De la gestión integral y control de riesgos", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero", de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capitulo V "De la gestión del riesgo operativo";

Que la norma contiene una serie de disposiciones especificas para la implementación de medidas de seguridad en los diferentes canales electrónicos a través de los cuales brindan servicios a sus clientes las instituciones financieras controladas por la Superintendencia de Bancos y Seguros;

Que del seguimiento trimestral del nivel de cumplimiento de las disposiciones contenidas en el citado capitulo V "De la gestión del riesgo operativo";,y del análisis de los resultados de las supervisiones in situ que ha venido realizando la Subdirección de Riesgo Operativo, se ha establecido la necesidad de realizar una reforma al referido capítulo V, con el propósito de que las instituciones financieras incrementen las medidas de seguridad en los canales electrónicos, mejoren los controles de gestión de la tecnología de la información y comunicaciones y mejoren la gestión del riesgo operativo; incluir disposiciones especificas relativas a la continuidad de las operaciones del negocio y la gestión de la seguridad de la información; e, implementar medidas de seguridad que mitiguen los fraudes relacionados con los cajeros automáticos y coadyuven a determinar los causales de los mismos en los procesos investigativos; y,

En uso de la atribución legal que le otorga la letra b) del artículo 175 de la Ley General de Instituciones del Sistema Financiero,

RESUELVE:

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero", de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar los siguientes cambios:

ARTÍCULO 1.- En el capitulo V "De la gestión del riesgo operativo", del titulo X "De la gestión y administración de riesgos", efectuar las siguientes reformas:

1. En todo el texto del capítulo V reemplazar la frase "... tecnología de información..." por "... tecnología de la información ...".

2. En el artículo 2, efectuar las siguientes reformas:

   2.1 Reemplazar el numeral 2.18, por el siguiente