UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

ESCUELA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN FINANCIERA

TRABAJO DE GRADO:

"PROPUESTA DE UN PLAN DE MITIGACIÓN PARA EL RIESGO OPERACIONAL EN INSTITUCIONES FINANCIERAS NO REGULADAS POR LA SUPERINTENDENCIA DEL SISTEMA FINANCIERO DE EL SALVADOR EN LA ZONA OCCIDENTAL"

PARA OPTAR AL GRADO DE:

MAESTRA EN ADMINISTRACIÓN FINANCIERA

PRESENTADO POR:

SANDRA KARINA CUELLAR, CC02082

KAREN LISSETTE GARCÍA RODRÍGUEZ, GR04014

DOCENTE DIRECTOR:

MAESTRO CESAR AUGUSTO SAGGETH ORTIZ

JULIO, 2017

SANTA ANA, EL SALVADOR, CENTROAMÉRICA

AUTORIDADES UNIVERSITARIOS

UNIDAD CENTRAL:

Rector: Maestro Roger Armando Arias

Vicerrector académico: Doctor Manuel De Jesús Joya

Vicerrector administrativo: Ingeniero Nelson Bernabé Granados

Secretario general: Maestro Cristóbal Ríos

Fiscal general: Licenciada Beatriz Meléndez

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE:

Decano: Maestro Raúl Ernesto Azcúnaga López

Vice-decano: Ingeniero Roberto Carlos Sigüenza

Secretario: Licenciado David Alfonso Mata Aldana

Administrador académico: Licenciado Herbert Rivas

Directora de la Escuela de

Posgrado: Maestra Rina Claribel Bolaños de Zometa

Coordinador de la Maestría en

Administración Financiera: Maestro Ricardo Misael Ayala Molina

Docente director: Maestro Cesar Augusto Saggeth Ortiz

Tribunal examinador: **Presidente:** Maestro Waldemar Sandoval.

Secretaria: Maestra Ana Silvia Guardado.

Vocal: Maestro Cesar Augusto Saggeth.

Agradecimientos

A Dios todopoderoso por regalarme la sabiduría y los recursos para culminar con éxito esta maestría.

A mi madre Carmen Cuellar, por su cariño, paciencia y apoyo incondicional siempre.

A mis hermanas Nancy y Marjorie por brindarme su apoyo.

A mis sobrinos: Alexis y Pamela por su apoyo y cariño.

A nuestro docente asesor master Saggeth, por su orientación, paciencia y dirección en el desarrollo de este trabajo.

A mi compañera de tesis Karen, por haber logrado nuestro objetivo con mucha perseverancia.

A los maestros y coordinadores de la Maestría en Administración Financiera de la escuela de postgrado de la Facultad Multidisciplinaria de Occidente, maestros Flor de María Rivera, Ana Silvia de Latín y Ricardo Ayala, por todo su apoyo y disposición.

A mis jefes maestro Julio Marroquín y Lcdo. Ever Peñalba y a todas las personas que nos ayudaron directa o indirectamente en el desarrollo de esta maestría.

Sandra Karina Cuellar

Agradecimientos

Le agradezco a Dios por haberme acompañado y guiado a lo largo de este proyecto, por ser mi fortaleza en momentos de debilidad y por brindarme un gran aprendizaje de vida con esta experiencia.

Le doy gracias a mi madre Patricia, por apoyarme en todo momento, por sus consejos y por haberme la oportunidad de formarme profesionalmente.

Le agradezco a mi compañera de grupo Karina, por ser una excelente compañera de equipo, amiga y apoyo, por motivarme a seguir adelante.

Gracias a nuestro docente director, maestro Saggeth, por brindarnos la oportunidad de acompañarnos y guiarnos en este proyecto.

Gracias a los coordinadores de la Maestría en Administración Financiera de la escuela de postgrado de la Facultad Multidisciplinaria de Occidente, los maestros Flor de María Rivera, Ana Silvia de Latín y Ricardo Ayala, por todo su apoyo y disposición.

Gracias a docentes que nos compartieron sus conocimientos en cada una de los cursos recibidos y a nuestros compañeros de la clases por todos los momentos de estudio, clases, tareas, desvelos, apuros, pero sobre todo por la buena amistad que iniciamos y conservamos.

Karen Lissette García Rodríguez

Resumen

En el Salvador las instituciones financieras son parte vital de la economía, pero gran parte de la población no tiene acceso al sistema financiero tradicional, por esta razón se estudia el tema de las instituciones financieras no supervisadas por Superintendencia del Sistema Financiero de El Salvador en el Occidente del país. Además se presentan generalidades del problema de investigación, en el que se establecen los propósitos, conveniencia, así como los antecedentes del sistema financiero en El Salvador,

Así mismo se detallan aspectos teórico relativos al riesgo operacional, tales como: definición, datos generales, importancia, marco regulatorio, factores y eventos de riesgo operacional, herramientas para la identificación, medición control y mitigación por medio de indicadores de riesgo operacional, aplicables a las instituciones objeto de estudio.

Se identifica la situación actual de la muestra tomada de las instituciones estudiadas, quienes en la actualidad no cuentan con una noción clara de los numerosos riesgos que a los que están expuestos, especialmente en un entorno que es cada vez más competitivo, de rápido crecimiento y poca regulación. Además se desarrolla y presenta la recolección, análisis y tabulación de los datos recopilados por la encuesta para reflejar cómo se maneja en la actualidad el riesgo operacional en las instituciones tomadas como muestra, que herramientas utilizan y si tienen personal asignado para realizar esas actividades.

Una parte importante del presente trabajo de grado es la propuesta, que está compuesta de un plan de mitigación para el riesgo operacional en instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental, así como también, se presenta como un complemento de nuestra propuesta, un plan de continuidad del negocio.

Contenido

Capitulo III: Metodología de investigación, diagnóstico y análisis de los resultados.

24

Índice de Ilustraciones

Índice de tablas y gráficas

Introducción

La gestión de riesgo operacional no es algo nuevo, sino que siempre ha sido una parte importante del esfuerzo de las entidades ya que toda empresa está expuesta a errores, fraudes, desastres naturales, fallas de los sistemas entre otras situaciones que pueden afectarles y generarles perdidas económicas importantes o incluso llevarlas a la quiebra.

En el sector financiero es muy importante la mitigación del riesgo operacional ya que este es inherente a las operaciones financieras, por tal razón en El Salvador existe la Superintendencia del Sistema Financiero, la cual es una entidad creada para supervisar y regular el sistema financiero para preservar su estabilidad, todo en concordancia con las mejores prácticas internacionales; dicha entidad excluye a toda institución de intermediación financiera que no cumpla con los requisitos mínimos para ser supervisados.

Por esta razón nace el propósito de este trabajo de grado, el cual es brindar herramientas a través de un plan de mitigación de riesgo operacional a las Instituciones Financieras no Supervisadas por la Superintendencia del Sistema Financiero de El Salvador en el Occidente, el cual consiste en un conjunto de actividades y estrategias necesarias para identificar, medir, mitigar y controlar los riesgos que pueden afectar al normal desarrollo de los procesos y el logro de objetivos y garantizara el resguardo de los fondos de sus asociados.

Adicionalmente en este trabajo se incluirá un plan de continuidad del negocio que permitirá identificar los procesos críticos para la institución y establecer una política de recuperación ante un desastre.

Capítulo I: Generalidades

En el capítulo I, presentamos generalidades del problema de investigación, en el que establecemos los propósitos de la investigación, la conveniencia, la trascendencia y las restricciones del estudio, así mismo como los antecedentes del sistema financiero en El Salvador, enfocándonos específicamente en las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador que conforman el sistema financiero paralelo a la banca tradicional, que son nuestro objeto de estudio.

1.1 Antecedentes

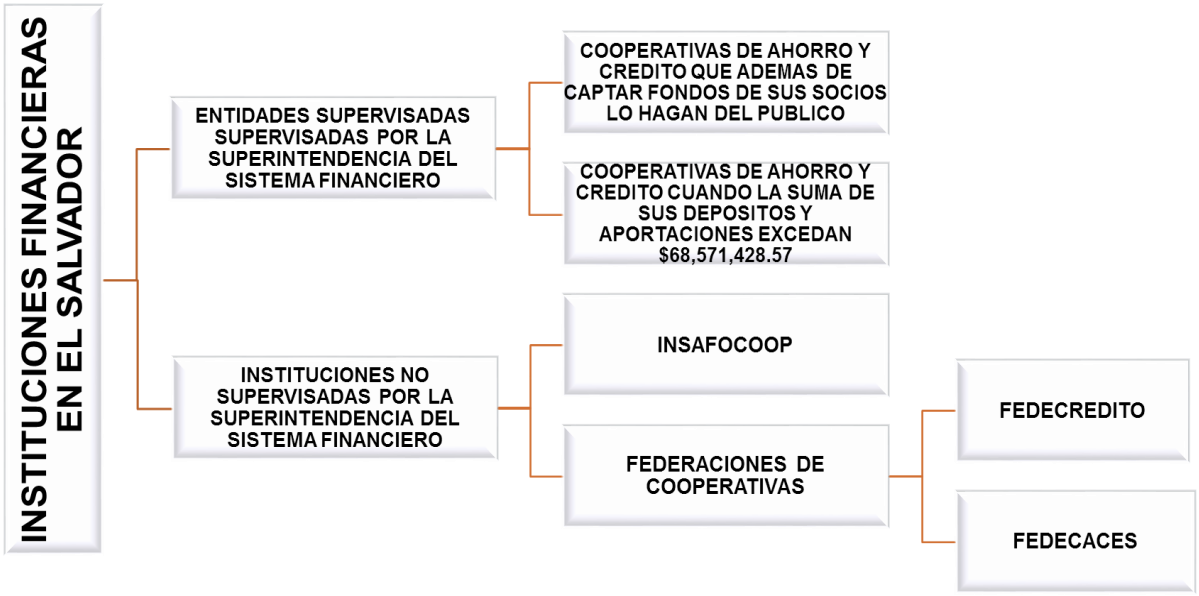
1.1.1 Instituciones financieras en El Salvador.

Las instituciones financieras son organizaciones que actúan como intermediarios financieros facilitando servicios financieros a sus clientes o miembros y se especializan en la acumulación de capitales y su transferencia por medio de préstamos a intereses. Son los responsables de transferir fondos desde los inversores hasta las empresas o personas que necesitan esos fondos. Éste tipo de instituciones se puede clasificar en tres grupos principales, tales como:

- "Entidades que toman depósitos, aceptándolos y gestionándolos, así como realizando a su vez préstamos; entre ellas se encuentran los Bancos tradicionales y las cooperativas de ahorro y créditos.
- Empresas de Seguros y Fondos de Pensiones.
- Corredores y Fondos Comunes de Inversión." (Siklos, 2001)

Los bancos son las instituciones financieras más conocidas y basan sus operaciones en la captación de ahorro y otorgamiento de crédito.

Ilustración N°1: Instituciones financieras en El Salvador



Elaborado por: Las autoras. Fuente: Superintendencia del Sistema Financiero de El Salvador, INSAFOCOOP, FEDECRÉDITO y FEDECACES.

1.1.2 Instituciones reguladas y sus normativas.

En El Salvador las Instituciones Financieras son supervisadas por la Superintendencia del Sistema Financiero y están reguladas por leyes como la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito de El Salvador, entre otras. La Superintendencia es parte del Sistema de Supervisión y Regulación Financiera que tiene por objeto preservar la estabilidad del sistema financiero y velar por la eficiencia y transparencia del mismo, así como velar por la seguridad y solidez de los integrantes del sistema financiero salvadoreño, entre las instituciones financieras reguladas por dicha institución están:

- “Los bancos cooperativos, que comprenden: Las cooperativas de ahorro y crédito que además de captar dinero de sus socios lo hagan del público y las cooperativas de ahorro y crédito cuando la suma de sus depósitos y aportaciones excedan seiscientos millones de colones o su equivalente en dólares: sesenta y ocho millones, quinientos setenta y un mil, cuatrocientos veintiocho 57/100 dólares.
- Las sociedades de ahorro y crédito.
- Las federaciones de Bancos Cooperativos calificadas por la Superintendencia para realizar con sus afiliados las operaciones de intermediación que señala la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito”. (Superintendencia del Sistema Financiero de El Salvador, 2016)

1.1.3 Las instituciones financieras no reguladas en El Salvador.

Las Instituciones Financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador están dedicadas a fortalecer el desarrollo y la integración financiera del país, asimismo están orientadas a la captación de pequeños ahorros y capitales y al financiamiento de micros, pequeñas y medianas empresas en los sectores rurales y urbanos.

Dichas instituciones financieras no reguladas, se están convirtiendo cada vez más en un segmento importante dentro del sistema financiero del país, el crecimiento de ellas conlleva la promesa de un sector financiero amplio y equilibrado, sin embargo necesitan de la creación y adopción de una estructura política coherente y de un sano ambiente de regulación y supervisión para su desarrollo y sostenibilidad.

1.1.3.1 *¿Que implica que una institución financiera no sea regulada y bajo que normativa operan?*

Que una institución financiera no sea regulada implica un mayor nivel de riesgo, ya que no se aplican los mismos principios de supervisión que a las instituciones financieras que captan dinero de sus socios y además lo hacen del público. En nuestro país se les llama no reguladas a las instituciones financieras que no cumplen los requisitos mínimos para ser supervisadas por la Superintendencia del Sistema Financiero de El Salvador, esto de acuerdo a lo descrito en el Art.2 de la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito , pero si se rigen para su constitución y operación bajo las normativas establecidas en el Código de Comercio y la Constitución de la Republica de El Salvador, así como también cuentan con la supervisión del INSAFOCOOP (Instituto Salvadoreño de Fomento Cooperativo) y de la Federación de Cooperativa de Ahorro y Crédito a la que se encuentren afiliadas.

1.1.3.1.1. INSAFOCOOP.

El Instituto Salvadoreño de Fomento Cooperativo se creó como corporación de Derecho Público, con autonomía en los aspectos económicos y administrativos. Entre las atribuciones que corresponden al INSAFOCOOP están:

- "La ejecución de la Ley General de Asociaciones Cooperativas;
- Iniciar, promover, coordinar y supervisar la organización y funcionamiento de las asociaciones cooperativas, federaciones y confederaciones de las mismas y prestarles el asesoramiento y asistencia técnica que necesiten;
- Planificar la política de fomento y desarrollo del cooperativismo para lo cual podrá solicitar la colaboración de los organismos estatales, municipales y particulares interesados en estas

actividades, a fin de que el movimiento cooperativista, se enmarque dentro de los programas de desarrollo económico del país;

- Conceder personalidad jurídica, mediante la inscripción en el Registro Nacional de Cooperativas, a las asociaciones cooperativas, federaciones de cooperativas y a la Confederación Nacional de Cooperativas;
- Conocer de la disolución y liquidación de las asociaciones cooperativas, federaciones y de la Confederación Nacional de Cooperativas;
- Ejercer funciones de inspección y vigilancia sobre las asociaciones cooperativas, federaciones de cooperativas y Confederación Nacional de Cooperativas, e imponer a las mismas las sanciones correspondientes
- Promover la creación e incremento de las fuentes de financiamiento de las asociaciones cooperativas, federaciones de cooperativas y Confederación Nacional de Cooperativas;
- Divulgar los lineamientos generales de actividad cooperativista, en particular los relativos a la administración y legislación aplicables a aquellas, con el objeto de promover el movimiento cooperativo;
- Asumir la realización o ejecución de programas o actividades que en cualquier forma y directamente se relacione con las atribuciones indicadas en el presente artículo". (Ley de Creación del Instituto Salvadoreño de Fomento Cooperativo, 1969)

1.1.3.1.2 Federaciones de cooperativas de ahorro y crédito en El Salvador.

"Las federaciones tendrán como objeto fundamental propiciar el desarrollo de un sistema de cooperativas de ahorro y crédito eficiente, solvente y competitivo, dedicado a la prestación de servicios financieros en áreas urbanas y rurales principalmente para familias de bajos y medianos

ingresos, y para la micro, pequeña y mediana empresa de los diferentes sectores económicos. Al efecto corresponde a las federaciones:

- Asesorar y capacitar a los bancos cooperativos para su mejor desempeño como afiliado de la federación, para el debido cumplimiento de ley y para desempeñarse como intermediarias financieras eficientes, competitivas y solventes.
- Actuar como caja central para apoyar a las cooperativas miembros en la administración de su liquidez.
- Intermediar recursos de instituciones públicas de crédito a sus afiliadas.
- Intermediar recursos de líneas de créditos de otras fuentes.
- Utilizar sus recursos disponibles para contribuir a la estabilización, crecimiento y desarrollo de sus afiliados.” (Ley de Bancos Coorporativos y Sociedades de Ahorro y Crédito, 2011)

A continuación se describen las Federaciones de Cooperativas de ahorro y crédito en El Salvador:

FEDECREDITO

Es “una entidad técnica que asocia a las cajas de crédito y a los bancos de los trabajadores, proporcionándoles servicios financieros, asistencia técnica, asesoría y servicios complementarios, de calidad; propiciando la integración, desarrollo sostenible, competitividad, alcance y cobertura” (Federación de cajas de creditos y de bancos de los trabajadores, s.f.).

En FEDECRÉDITO, se tiene un Pacto Social establecido donde expresa que "la Federación tiene como objeto fundamental propiciar el desarrollo de un Sistema de Cooperativas de Ahorro y Crédito eficiente, solvente y competitivo, dedicado a la prestación de servicios financieros en áreas

urbanas y rurales principalmente a familias de bajos y medianos ingresos y a las micro, pequeñas y medianas empresas de los diferentes sectores económicos, así como a los trabajadores públicos, municipales y privados", por esta razón es que se elabora todo un proceso de planificación estratégica e implementan una ejecución efectiva de los diferentes planes, que le permite estar a la vanguardia del Sistema, promoviendo el crecimiento y desarrollo, con prudencia y responsabilidad. "Instituciones afiliadas a FEDECREDITO en Occidente:

- SANTA ANA: Primer Banco de los Trabajadores de Santa Ana, Caja de Crédito de Candelaria de la Frontera, Caja de Crédito de Chalchuapa y Caja de Crédito de Santa Ana.
- AHUACHAPAN: Caja de Crédito de Ahuachapán y Caja de Crédito de Atiquizaya.
- SONSONATE: Banco Izalqueño de los Trabajadores, Caja de Crédito de Acajutla, Caja de Crédito de Armenia, Caja de Crédito de Izalco, Caja de Crédito de Juayúa y Caja de Crédito de Sonsonate". (Federación de cajas de creditos y de bancos de los trabajadores, s.f.)

FEDECACES

"La Federación de Asociaciones Cooperativas de Ahorro y Crédito de El Salvador de Responsabilidad Limitada, FEDECACES de R.L., es una entidad de segundo piso, fundada el 11 de junio de 1966, con 51 años, integra a más de 30 Cooperativas de Ahorro y Crédito, con presencia en los 14 Departamentos del país, atiende a diversos sectores de la población salvadoreña, sean trabajadores asalariados, privados o públicos, micro y pequeños empresarios, amas de casa y profesionales, entre otros.

FEDECACES provee servicios de apoyo a la liquidez en su Caja Central, intermediación financiera con créditos y ahorros, facilita las transferencias de remesas, Supervisión de autorregulación, soporte técnico informático; a todas las Cooperativas afiliadas, articulando sus 81

puntos de servicio a nivel nacional, a través de Red Activa". (Federación de Asociaciones Cooperativas de Ahorro y Crédito de El Salvador, s.f.)

1.1.4 Sistema bancario paralelo al sistema bancario tradicional.

"El Consejo de Estabilidad Financiera ha descrito recientemente al sistema bancario paralelo como el conjunto de instituciones y actividades de intermediación crediticia por fuera del sistema bancario tradicional, que llevan a cabo dicha intermediación en un marco en el cual, o no se aplican los estándares de regulación prudencial y de supervisión, o se ejercen en un grado diferente y en la práctica menos estricto que el aplicable a las instituciones bancarias normalmente dedicadas a actividades similares" (Consejo de Estabilidad Financiera, 2009).

Además el sistema paralelo es también conocido como el sistema bancario en la sombra, definido como el conjunto de instituciones financieras, infraestructura y prácticas que sustentan operaciones al margen de las regulaciones nacionales.

Los mercados de capitales y la banca en la sombra, se han convertido en los nuevos canales de financiamiento para el sector que no puede acceder al crédito bancario tradicional. Este sistema financiero en la sombra complementa al sistema bancario y a los mercados ordinarios, supliendo sus carencias y pudiendo financiar sectores económicos.

1.2 Planteamiento del problema

¿Cómo mitigar la ocurrencia de eventos derivados del riesgo operacional en relación a la frecuencia y severidad de las pérdidas, en instituciones financiera no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental?

1.3 Objetivos

1.3.1 Objetivo general.

Proponer un Plan de Mitigación para el Riesgo Operacional en Instituciones Financieras no Reguladas por la Superintendencia del Sistema Financiero de El Salvador en la Zona Occidental.

1.3.2 Objetivos específicos.

Identificar a las instituciones financieras no reguladas por la Superentendía del Sistema Financiero de El Salvador en la zona occidental, que conforman el objeto de estudio de nuestro trabajo de grado.

1.4 Justificación

Una de las principales preocupaciones de las instituciones financieras consiste en medir el riesgo de operacional en forma adecuada, como un proceso indispensable de garantía para los posibles inversionistas. Tomando en cuenta que riesgo operacional es la posibilidad de ocurrencia de pérdidas financieras, originadas por fallas o insuficiencias de procesos, personas, sistemas internos, tecnología y en la presencia de eventos externos imprevistos, la cual incluye el riesgo legal, pero excluye los riesgos sistemáticos y de reputación, así también no se toma en cuenta las pérdidas ocasionadas por cambios en el entorno político, económico y social.

En este sentido, la importancia de una adecuada gestión y supervisión del riesgo operacional para generar un efectivo desempeño y estabilidad en el sistema bancario, justifica y hace necesario la realización de un Plan de mitigación de riesgo enfocado en las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona

Occidental, ya que ellas no están reguladas por dicha entidad y están expuestas a un riesgo operacional el cual deben minimizar para asegurar en primer lugar su existencia y permanencia, su rentabilidad y desarrollo y la expansión y crecimiento haciéndolas cada vez más competitivas dentro del mercado.

Por lo que mantener una adecuada administración y supervisión del riesgo operacional es uno de los desafíos más grandes a los que se enfrentan las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, las cuales son de acuerdo al artículo 2 de la Ley de Bancos Cooperativas y Sociedades de Ahorro y Crédito: Asociaciones Cooperativas de Ahorro y Crédito, Sociedades Cooperativas de Ahorro y Crédito (Cajas de Crédito / Banco de los trabajadores) y las Sociedades Financieras no Cooperativas.

Este Plan pretende modelar las variables cualitativas y cuantitativas que explican las pérdidas operativas mediante la identificación de los factores de complejidad del negocio que exponen a la entidad y que permiten medirlos con el propósito de ayudar a la toma de decisiones, tomando para ellos la metodología de control de riesgo operacional aplicado según la normativa de la Superintendencia del Sistema Financiero de El Salvador y así como los convenios de Basilea.

1.5 Alcances y limitaciones

1.5.1 Alcances.

Con la puesta en marcha de este plan de mitigación se logrará alcanzar optimización de recursos económicos, tiempo y esfuerzo, que tomaría invertir en caso de ocurrencia de eventos relacionados directamente con la gestión inadecuada del riesgo operacional de las instituciones, permitiendo de esta manera el uso de los recursos se enfoque en actividades que puedan generar

rentabilidad reduciendo la posibilidad de inconvenientes en el buen funcionamiento de las mismas, brindando así seguridad y confianza a sus propietarios, clientes y usuarios.

1.5.2 Limitaciones.

Éste proyecto se limita a las Instituciones Financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la Zona Occidental del país, que pretende ser una guía de apoyo para que dichas entidades puedan comenzar su camino en la gestión del riesgo operacional con la identificación de los riesgos operacional, como medirlos, controlarlos, para finalmente mitigarlos sustancialmente, basándose en la metodología de control de riesgo operacional aplicado según la normativa de la Superintendencia del Sistema Financiero de El Salvador y los convenios de Basilea; no así la aplicación práctica del plan en una institución especifica o en particular.

Capitulo II: Marco teórico

El capítulo II, contiene aspectos teórico relativos al Riesgo Operacional, tales como: definición, datos generales, importancia, marco regulatorio, factores y eventos de riesgo operacional, herramientas para la identificación, medición control y mitigación por medio de indicadores de riesgo operacional, aplicables a las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador.

2.1 El riesgo

"El Riesgo es una medida de la magnitud de los daños frente a una situación peligrosa. El riesgo se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro. Si bien no siempre se distingue adecuadamente entre peligrosidad (probabilidad de ocurrencia de un peligro), vulnerabilidad (probabilidad de ocurrencia de daños dado que se ha presentado un peligro) y riesgo propiamente dicho". (Gumercindo Ruíz, 2000)

2.1.1 Riesgos financieros

"El Riesgo financiero es la probabilidad de un evento adverso y sus consecuencias, se refiere a la probabilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para una organización. El concepto debe entenderse en sentido amplio, incluyendo la posibilidad de que los resultados financieros sean mayores o menores de los esperados. De hecho, habida la posibilidad de que los inversores realicen apuestas financieras en contra del mercado, movimientos de éstos en una u otra dirección pueden generar tanto ganancias o pérdidas en función de la estrategia de inversión" (Gumercindo Ruíz, 2000).

2.1.1.1 Tipos de riesgo financieros.

"La gestión de riesgo financiero ha cobrado una especial relevancia a nivel internacional, debido en parte a las crisis financieras de los años noventa. La gestión de riesgos financieros se ocupa de diversos tipos de riesgos financieros.

- **Riesgo de crédito:** Es la posibilidad de pérdida, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte, entendida esta última como un prestatario o un emisor de deuda.
- **Riesgo de mercado**: Es la posibilidad de pérdida, producto de movimientos en los precios de mercado que generan un deterioro de valor en las posiciones dentro y fuera del balance o en los resultados financieros de la entidad.
- **Riesgo de liquidez:** Es la posibilidad de incurrir en pérdidas por no disponer de los recursos suficientes para cumplir con las obligaciones asumidas, incurrir en costos excesivos y no poder desarrollar el negocio en las condiciones previstas.
- **Riesgo reputacional:** Es la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros.
- **Riesgo técnico:** Es la posibilidad de pérdidas por inadecuadas bases técnicas o actuariales empleadas en el cálculo de las primas y de las reservas técnicas de los seguros, insuficiencia de la cobertura de reaseguros, así como el aumento inesperado de los gastos y de la distribución en el tiempo de los siniestros.
- **Riesgo operacional:** Es la posibilidad de incurrir en pérdidas, debido a las fallas en los procesos, el personal, los sistemas de información y a causa de acontecimientos externos;

incluye el riesgo legal". (Norma para la Gestión del Riesgo Operacional de las Entidades Financieras, NPB4-50, 2012)

2.2 El riesgo operacional

"Basilea II, define el riesgo operacional como el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional. El Nuevo Acuerdo de Basilea complementa esta definición con una clasificación más detallada del tipo de eventos de pérdida, que sirve además como guía para delimitar una definición que es en sí muy amplia. El primer nivel enumera siete tipos de eventos que tienen la consideración de pérdida por riesgo operacional y proporciona una definición de los mismos" (Acuerdos de Basilea II, 2016). Las instituciones deberán asignar sus datos de pérdidas a cada una de las siguientes categorías:

Ilustración N°2: Categorías de Riesgo Operacional

Elaborado por: Las autoras. Fuente: Acuerdos de Basilea II

La gestión de riesgos operacional no es algo nuevo, sino que siempre ha sido una parte importante del esfuerzo de las instituciones por evitar el fraude, mantener la integridad de los controles internos, reducir los errores en las operaciones, etc. Para algunas instituciones era un concepto muy amplio, básicamente todo aquello que quedaba fuera del riesgo de crédito o de mercado, mientras que para otras era una acepción restringida a fallos operativos o de procesos.

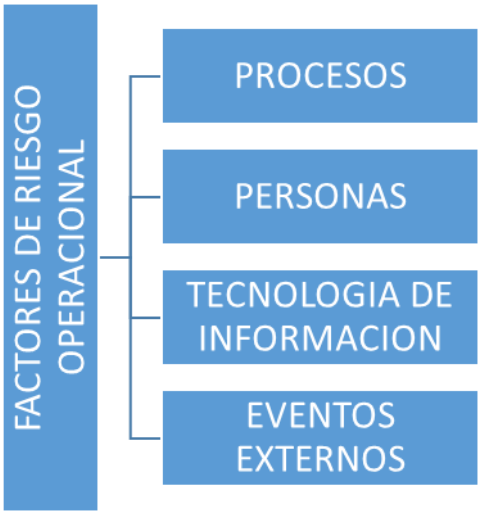
La entidad ha establecido un marco para la gestión del riesgo operacional que comprende las políticas, prácticas, procedimientos y estructura con que cuenta la entidad para su adecuada gestión. En este marco se definen, entre otros aspectos, los procedimientos que utilizará la unidad de riesgo operacional para evaluar la vulnerabilidad de la entidad ante la ocurrencia de eventos de pérdida, comprender su perfil de riesgo operacional y adoptar las medidas correctivas que sean pertinentes.

Dado que la efectiva gestión de este riesgo contribuye a prevenir futuras pérdidas derivadas de eventos operativos, la entidad no sólo gestiona el riesgo operacional inherente a productos, actividades, procesos y sistemas vigentes, sino también el correspondiente a nuevos productos, inicio de actividades, puesta en marcha de procesos o sistemas en forma previa a su lanzamiento o implementación.

2.2.1 Factores generadores o áreas críticas de riesgo operacional.

Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operacional. Son factores de riesgo operacional los procesos, las personas, la tecnología de información y los eventos externos.

Ilustración N°3: Factores de Riesgo Operacional



Elaborado por: Las autores. Fuente: Norma NPB4-50, para la gestión del riesgo operacional de las instituciones financieras.

2.2.1.1 Procesos.

"Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones deben contar con procesos documentados, definidos y actualizados permanentemente, que pueden ser agrupados en procesos estratégicos y operativos. Las instituciones deben gestionar apropiadamente los riesgos asociados a dichos procesos, con énfasis en las fallas o debilidades que presenten, dado que éstas pueden tener como consecuencia el desarrollo deficiente de las operaciones.

2.2.1.2 Personas.

Las instituciones deben establecer políticas, procesos y procedimientos que procuren una adecuada planificación y administración del capital humano, que incluyan el proceso de

contratación, permanencia y desvinculación del personal. Asimismo, deben establecer mecanismos preventivos que permitan identificar y gestionar fallas, insuficiencias, negligencia, sabotaje, robo, inadecuada capacitación, apropiación indebida de información, entre otros, asociadas al personal, vinculado directa o indirectamente a la institución; de tal modo que se minimice la posibilidad de pérdidas económicas.

La vinculación directa es aquélla que está basada en un contrato interno de trabajo, de acuerdo a la legislación laboral respectiva. La vinculación indirecta está referida a aquellas personas que tienen una relación jurídica con la entidad para la prestación de determinados servicios, diferente de aquélla que se origina de un contrato interno de trabajo.

2.2.1.3 Tecnología de información.

Las instituciones deben gestionar los riesgos asociados a la tecnología de información, los relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como la calidad de la información y una adecuada inversión en tecnología.

2.2.1.4 Eventos externos.

Las instituciones deben gestionar los riesgos asociados a eventos externos ajenos al control de la institución que pudiesen alterar el desarrollo normal de sus actividades relacionados a fallas en los servicios críticos provistos por terceros, contingencias legales, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores". (Norma para la Gestión del Riesgo Operacional de las Entidades Financieras, NPB4-50, 2012)

2.3 Administración de riesgo operacional

La administración del riesgo operacional, es la disciplina que combina los recursos financieros, humanos, materiales y técnicos de una empresa, para identificar o evaluar los riesgos potenciales y decidir cómo manejarlos con la combinación optima de costos-efectividad. Visto desde un marco amplio implica que las estrategias, procesos, personas, tecnología de información y conocimientos estén alineados para manejar toda la incertidumbre que una institución enfrenta. El manejo del riesgo permite establecer parámetros aceptables de exposición al riesgo, eliminando actividades o prácticas que pongan en peligro la continuidad de la operación. La administración de riesgo permite a la alta dirección de una institución tomar decisiones con conocimiento del riesgo y no basados en el azar de los eventos.

2.3.1 Beneficios de la administración de riesgo operacional.

Los beneficios que permite la administración de riesgo es identificar los activos empresariales que están en máximo riesgo, valuar las vulnerabilidades y los impactos potenciales y proponer resguardos y tácticas de mitigación, lo que permitirá:

- Priorizar y establecer niveles de riesgo para sus procesos y recursos empresariales críticos.
- Pasar de un enfoque de mitigar el riesgo a prevenir proactivamente las fallas.
- Tomar decisiones más informadas sobre cómo proteger su empresa.
- Evaluar las tácticas y los costos de la administración de riesgos relacionados con los diferentes niveles de protección.
- Prepararse adecuadamente para las auditorías de las agencias de control.

2.3.2 Etapas de la gestión del riesgo operacional.

Para la gestión del riesgo operacional las instituciones deben contar con un proceso continuo y documentado de cada una de sus etapas, las cuales se detallan a continuación:

2.3.2.1 Identificación.

"La identificación efectiva del riesgo considera tanto los factores internos como externos que podrían afectar adversamente el logro de los objetivos institucionales. Las instituciones deben establecer su mapa de riesgo operacional a través de un proceso de identificación de todos sus eventos de riesgos operacionales, es conveniente que la identificación de los eventos pueda agruparse, adicionalmente, de acuerdo a las líneas de negocio que la entidad mantiene." (Salinas Zhunio, 2012)

2.3.2.2 Medición

"Las instituciones deben estimar o cuantificar el riesgo operacional considerando la probabilidad de ocurrencia y el impacto económico en los resultados de la entidad. Esta cuantificación es esencial para la entidad porque en función a ellas se establecen las medidas de control y mitigación que buscan minimizar pérdidas por este riesgo. Las metodologías y herramientas para estimar o cuantificar el riesgo operacional deben estar de conformidad con el tamaño, naturaleza de los niveles de riesgos asumidos por la entidad y volumen de sus operaciones." (Salinas Zhunio, 2012)

2.3.2.3 Control.

"Se refiere a las acciones o mecanismos de cobertura y control implementados por la institución con la finalidad de prevenir o reducir los efectos negativos en caso de materializarse los eventos adversos de riesgo operacional.

2.3.2.4 Mitigación.

Mitigar significa reducir o eliminar el riesgo, una vez conocida la importancia de cada factor de riesgo operacional, debemos proceder a la mitigación de aquéllos que pueden ser relevantes. Es necesario establecer un plan de acción para implementar medidas que busquen mitigar los eventos de riesgo identificados. Este plan debe detallar las acciones a implementar, el plazo estimado de ejecución y los responsables directos de dicha ejecución." (Salinas Zhunio, 2012)

2.3.2.5 Monitoreo y comunicación.

"Las instituciones deben dar seguimiento sistemático y oportuno a los eventos de riesgo operacional, así como a los resultados de las acciones adoptadas. El seguimiento deberá asegurar una revisión periódica y la generación de información suficiente para apoyar los procesos de toma de decisiones. Las instituciones deben realizar un monitoreo permanente de su mapa de riesgos y exposición a pérdidas por riesgo operacional, debiendo cumplir como mínimo con los siguientes aspectos:

- Desarrollar procesos de seguimiento efectivo y permanente que permitan la rápida detección y corrección de las deficiencias
- Establecer indicadores que evidencien potenciales riesgos operacionales

- Asegurar que los controles internos establecidos se encuentren funcionando en forma efectiva y eficiente.
- Asegurar que los riesgos residuales se encuentren bajo el nivel de tolerancia establecido por cada institución.

La institución debe contar con sistemas de información gerencial y bases de datos estadísticas que posibiliten la generación de información oportuna, confiable, consistente y homogénea para los reportes periódicos a la Junta Directiva, Comité de Riesgos y/o Alta Gerencia, así como a otros interesados responsables de la toma de decisiones en la gestión del riesgo operacional." (Salinas Zhunio, 2012)

2.4 Plan de mitigación de riesgo operacional

El Plan de Mitigación de Riesgo Operacional, es el resultado de un conjunto de actividades y estrategias necesarias para identificar, medir, mitigar y controlar los riesgos que pueden afectar al normal desarrollo de los procesos y el logro de objetivos. De igual forma, establece acciones inmediatas y otras de carácter preventivo que deben ejecutarse para controlar o prevenir los eventos generadores de riesgo ocasionados por factores internos o externos que involucren a procesos, personas y sistemas.

2.4.1 Objetivo del plan de mitigación de riesgo operacional.

El objetivo de un plan de mitigación de riesgo operacional, es disminuir la probabilidad de ocurrencia de riesgos de tipo operacional que puedan ocasionar un impacto negativo en el desarrollo de las actividades diarias de las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental, así como, contribuir

a la efectividad de los controles para minimizar la exposición de la institución ante factores de riesgo, de manera que se garantice la continuidad de las operaciones.

2.5 Relación del riesgo operacional con otros tipos de riesgo y su aplicación en las instituciones financieras no reguladas

"El riesgo operacional no es un riesgo nuevo, de hecho, es un riesgo inherente a cualquier negocio y no es exclusivo de la actividad financiera. Sin embargo, la preocupación por este riesgo ha crecido considerablemente en los últimos años, tanto por parte de las instituciones financieras como por parte de otro tipo de empresas.

El riesgo operacional o de negocio se deriva de las decisiones que se toman diariamente dentro de una institución, en el caso de las instituciones financieras se pueden mencionar las decisiones en cuanto a transacciones, asignación de tasas, otorgamiento de créditos, aprobación de créditos y sus desembolsos, controles internos, contratación de personal, entre otras., todas estas actividades involucran otros tipos de riesgos, entre ellos principalmente el riesgo de mercado y riesgo de crédito. Estos tipos de riesgos suelen ser muy difíciles de separar del riesgo operacional ya que este va enlazado en la mayoría de las situaciones que se generan en las actividades diarias de la institución.

Algunos ejemplos de prácticas o actividades que pueden generar riesgos son: los accesos no autorizados, fraudes a empleados, obsolescencia del sistema, ausencia de gestión experta, riesgo del proveedor de servicio, el cliente no cumple las pautas de seguridad y el cliente niega haber realizado la transacción. Por esta razón es vital para las instituciones financieras que no son supervisadas por la Superintendencia del Sistema Financiero que conozcan y retomen algunas prácticas de controles para poder mitigar el riesgo en sus operaciones." (Salinas Zhunio, 2012)

Capitulo III: Metodología de investigación, diagnóstico y análisis de los resultados.

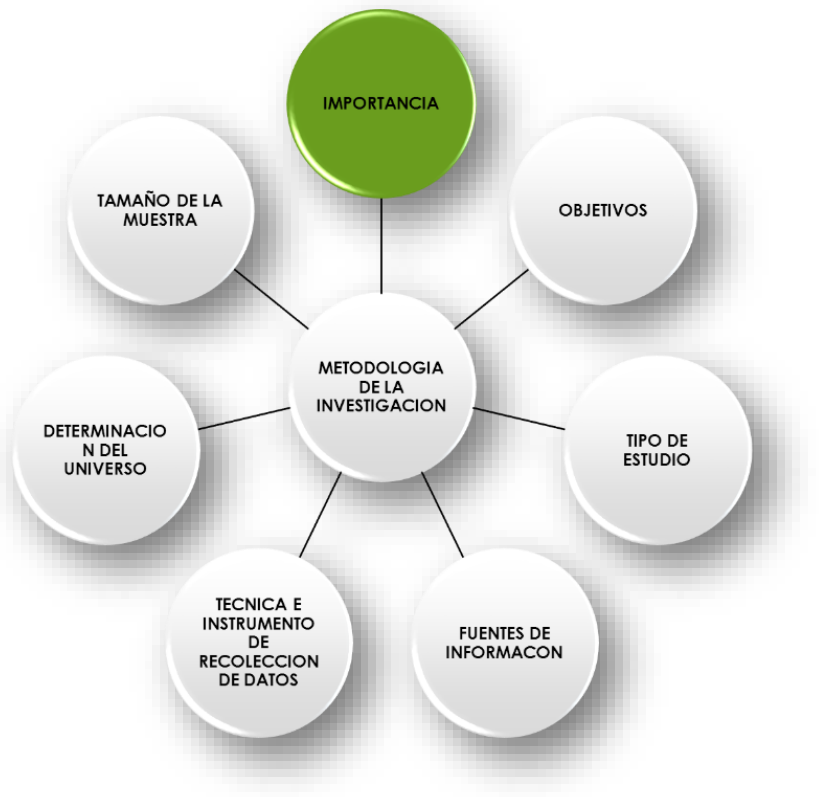
En el capítulo III presentamos la situación actual de la muestra tomada de las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental, quienes en la actualidad no cuentan con una noción clara de los numerosos riesgos que a los que están expuestos, especialmente en un entorno que es cada vez más competitivo, de rápido crecimiento y poca regulación.

Además se desarrolla y presenta la recolección, análisis y tabulación de los datos recopilados por la encuesta para reflejar cómo se maneja en la actualidad el riesgo operacional en las instituciones tomadas como muestra, que herramientas utilizan y si tienen personal asignado para realizar esas actividades.

3.1 Metodología de la investigación

Nos ayudará en el proceso de adquirir conocimientos para elaborar, definir y sistematizar el conjunto de técnicas, métodos y procedimientos que se seguirán durante el desarrollo de la de investigación.

Ilustración N°4: Metodología de la investiga



Elaborado por: Las autoras. Fuente: Libro Metodología de la investigación de Roberto Hernández Sampieri. 6ta. edición.

3.1.1 Importancia de la investigación.

Las instituciones Financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en el Occidente del país, requieren una oportuna gestión y supervisión de Riesgo Operacional que garantice la continuidad de la operación de dichas instituciones, ya que éstas representan un pilar fundamental en la economía salvadoreña al ser quienes ofrecen servicios de intermediación financiera al sector poblacional que no tiene acceso al sistema financiero o banca tradicional.

Por esta razón estas instituciones financieras no reguladas deben obtener una estabilidad que les permita brindar a sus clientes y asociados productos y servicios de confianza, agilidad, exactitud, cortesía y responsabilidad.

3.1.2 Objetivos de la investigación.

3.1.2.1 Objetivo general.

Identificar la manera en que las instituciones financieras no Supervisadas por la Superintendencia del Sistema Financiero ubicadas en la zona occidental de El Salvador administran el Riesgo Operacional en sus actividades de intermediación financiera.

3.1.2.2 Objetivos específicos.

- Determinar el nivel de gestión de riesgo operacional que actualmente despliegan las instituciones en estudio, por medio de la identificación, medición, mitigación y control del mismo.
- Identificar de qué manera las instituciones financieras objeto del presente estudio consideran los factores de riesgo internos y externos del sector.
- Establecer, si el seguimiento que las instituciones objeto de estudio realizan sobre el riesgo operacional, es eficaz en la detección y corrección de deficiencias que puedan convertirse en acontecimientos de éste tipo de riesgo.
- Comprobar si las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental, cuentan con políticas y procesos de control para asegurar un óptimo desempeño de sus operaciones y que garanticen la continuidad del negocio.

- Determinar si las instituciones objeto de éste estudio, cuentan con un plan de continuidad del negocio acorde al tamaño y complejidad de la sus operaciones.

3.1.3 Tipo de estudio.

El estudio es de tipo descriptivo, debido a que se concentra en investigar y describir la problemática que las Instituciones Financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la Zona Occidental, tienen para mitigar el Riesgo Operacional, dicha problemática a la vez permitirá proponer un Plan de Mitigación para Riesgo Operacional, así como un Plan de Continuidad del negocio que les permita desempeñarse eficientemente previniendo posibles eventos de riesgo.

3.1.4 Fuentes de información.

3.1.4.1 Fuentes primarias.

Los datos primarios de la investigación se obtuvieron mediante la técnica de la encuesta, utilizando el cuestionario como instrumento para recopilarlos y así dar respuesta a los objetivos presentados en la misma. Esto permitirá contar con información confiable y válida.

3.1.4.2 Fuentes secundarias.

Las principales fuentes secundarias de información de esta investigación lo conforman libros de texto relacionados con las variables en estudio, así como leyes, memorias de labores, revistas económicas publicadas por diferentes asociaciones privadas relacionadas con servicios financieros, sitios Web y otras fuentes no menos importantes a los fines de la investigación.

3.1.5 Técnica e instrumento de recolección de la información.

La investigación fue desarrollada mediante el uso la Encuesta como técnica y el cuestionario como instrumento para la recolección de datos.

3.1.5.1 Cuestionario.

El cuestionario está compuesto por una serie de preguntas cerradas, abiertas y de opción múltiple, todas relacionadas con el objeto de estudio, mismo que será completado por el personal de mandos medios o gerentes de las instituciones tomadas como muestra y los datos recolectados serán tabulados y posteriormente analizados.

3.1.6 Determinación del universo.

El tema de investigación delimita como población de estudio a las Instituciones Financieras no Supervisadas por la Superintendencia en el Occidente de El Salvador, las cuales son en total cincuenta y tres instituciones de éste tipo, divididas en doce Cajas de Crédito afiliadas a FEDECREDITO y cuarenta y un Asociaciones Cooperativas de Ahorro y Crédito afiliadas al INSAFOCOOP.

3.1.6.1 Tamaño de la muestra.

Tomando en cuenta que la muestra es una representación significativa de las características de la población, se han tomado seis instituciones financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador la zona Occidental, las cuales se seleccionaron en una muestra aleatoria simple que se considera representativa para los fines de la investigación, dado que se pueden agrupar en dos grandes sectores, por un lado están las

asociaciones cooperativas de ahorro y crédito y por otro las cajas de crédito, cada una de las instituciones que pertenecen a un determinado sector tienen un modelo de negocio muy similar, por lo que comparten características homogéneas respecto a la administración.

3.1.7 Administración de datos de la encuesta.

La encuesta está dirigida a Mandos medios o Jefaturas de instituciones financieras no reguladas por Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, en su ausencia se encuestará al Gerente General.

Ilustración N°5: Administración de datos

Elaborado por: Las autoras. Fuente: Libro Metodología de la investigación de Roberto Hernández Sampieri. 6ta. edición.

3.1.7.1 Tabulación y análisis de datos.

Los resultados de la encuesta serán tabulados por cada una de las preguntas del cuestionario y posteriormente representados gráficamente por respuesta para facilitar su interpretación y análisis. Esto permitirá identificar algunos elementos adicionales que muestren las debilidades actuales y así enriquecer la propuesta de Plan de Mitigación de Riego Operacional y complementado por un Plan de continuidad del negocio. A continuación se presenta la estructura que tendrán los cuadros de tabulación y análisis de datos:

- Pregunta: Se presentará la pregunta exactamente como se planteó en el cuestionario.
- Cuadro de frecuencia y gráficos: En el cuadro de tabulación de datos se detallarán los resultados de la pregunta formulada e incluye el gráfico correspondiente.
- Análisis e Interpretación de Datos: Con los resultados obtenidos por pregunta se procederá a realizar el análisis e interpretación de los mismos, los cuales se convertirán en el insumo principal para formular el análisis.

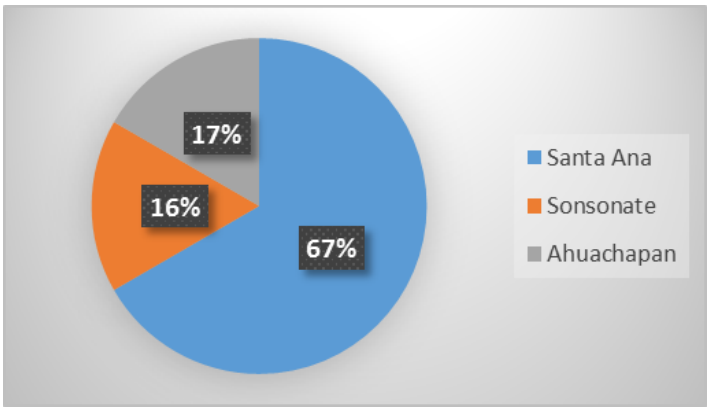
3.1.7.2 Presentación de resultados e interpretación de datos y gráficos.

Ubicación Geográfica de las Instituciones Financieras encuestadas

Tabla N1: Tabulación de datos, sobre la ubicación geográfica de las Instituciones Financieras encuestadas

RESPUESTAS		
Santa Ana	**Sonsonate**	**Ahuachapan**
67%	17%	17%

Gráfica N°1: Representación gráfica de datos, sobre la ubicación geográfica de las Instituciones Financieras encuestadas



La muestra seleccionada para el estudio es de seis Instituciones no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona de Occidente, la cual se encuentra conformada por los departamentos de Santa Ana, Sonsonate y Ahuachapán. En el Departamento de Santa Ana está la mayor concentración de instituciones por lo que como resultado de la selección aleatoria de la muestra, se obtuvieron cuatro instituciones en éste departamento; En Sonsonate se encuestó una institución y una en el departamento de Ahuachapán.

3.1.7.2.1 Instituciones financieras no reguladas por la superintendencia del sistema financiero de El Salvador, en la zona occidental, encuestadas.

- Caja de Crédito de Santa Ana – FEDECRÉDITO – STA.ANA

- Caja de Crédito de Candelaria de la Frontera - FEDECRÉDITO – STA.ANA

- Caja de Crédito de Juayúa – FEDECRÉDITO- SONSONATE

- FINCA MICROFINANZAS, S.A. DE C.V. – AHUACHAPAN

- SIHUACOOP DE R.L. – STA.ANA

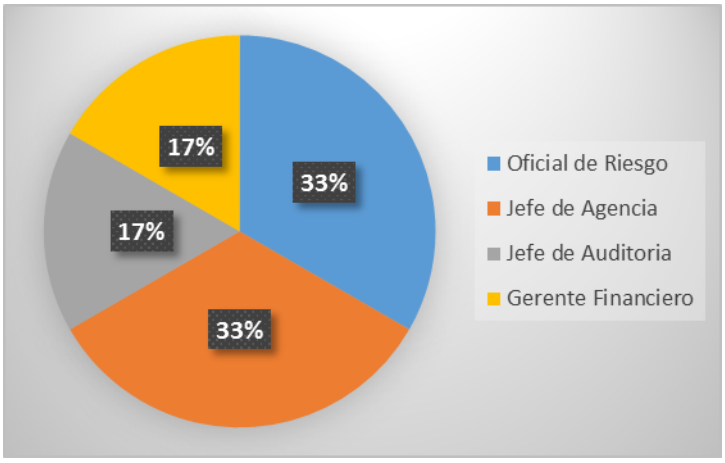
- COOP-1 DE R.L. – STA.ANA

3.1.7.3. Perfil encuestado.

Tabla N°2: Tabulación de datos sobre el perfil encuestado

RESPUESTAS			
Oficial de Riesgo	**Jefe de Agencia**	**Jefe de Auditoria**	**Gerente Financiero**
33%	33%	17%	17%

Gráfica N° 2: Representación gráfica de datos sobre el perfil encuestado



De la muestra encuestada solamente el 33% son Oficial de Riesgo debido a que las demás instituciones no cuentan con esta posición, lo que los obliga a distribuir estas actividades en personal de otros puestos como los son Jefes de Agencia, Jefe de Auditoria o Gerente Financiero, quienes nos atendieron para responder los cuestionarios.

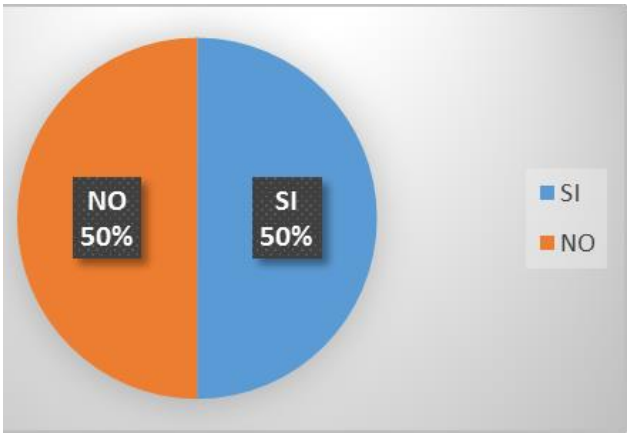
3.1.7.4 Desarrollo del cuestionario y análisis de los resultados.

Pregunta N°1. ¿La institución financiera cuenta con la posición de Oficial de Riesgo o con un responsable de Administrar el riesgo?

Tabla N° 3: Tabulación de datos resultados de cuestionario, pregunta N°1.

RESPUESTAS	
SI	NO
50%	50%

Grafico N°3: Representación gráfica de los resultados de cuestionario, pregunta N°1



El 50% de las instituciones manifiesta que cuentan con encargados de gestionar todo tipo de riesgo, incluyendo el riesgo operacional, la mayoría lo denominan Oficial de Riesgo, en otra

institución lo denominan Comité de Riesgos el cual está conformado por Asociados de la misma, otras instituciones mencionan que se apoyan en una jefatura a quien le han asignado dentro de sus responsabilidades gestionar el riesgo.

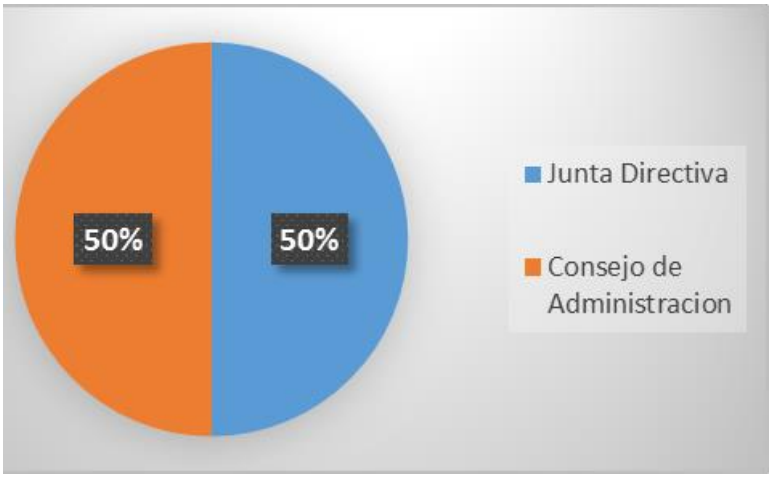
El 50% restante expresan que no cuentan con un responsable directo de la administración del Riesgo, que esté asignado exclusiva o primordialmente a la gestión de riesgos, lo que lleva por consecuencia no tener una persona enfocada en esta actividad y por esta razón se consideran que están más expuestas a la ocurrencia de eventos de todo tipo de Riesgo.

Pregunta N°2. ¿De quién dependen Jerárquicamente la o las personas responsables de la gestión del riesgo operacional?

Tabla N° 4: Tabulación de datos resultados de cuestionario, pregunta N°2

RESPUESTAS	
Junta Directiva	**Consejo de Administracion**
50%	50%

Grafico N°4: Representación gráfica de los resultados de cuestionario, pregunta N°2



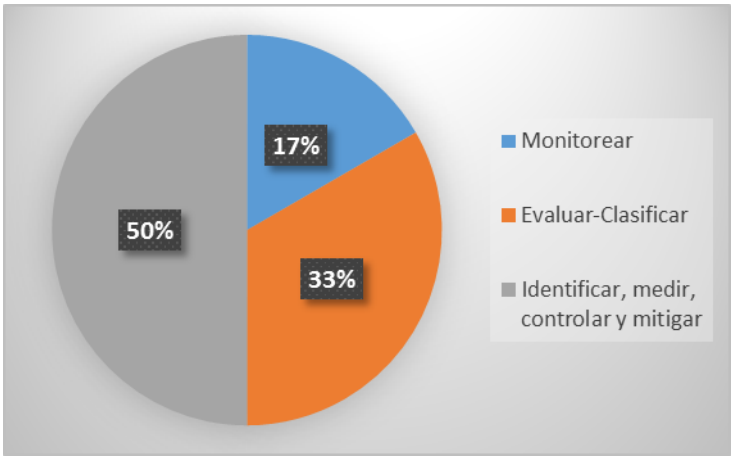
El 50% de los encuestados manifestaron que sus encargados de administrar el Riesgos dependen jerárquicamente de la Junta Directiva, por lo que deben de rendir cuentas a ellos. El restante 50% reportan al Consejo de Administración quien es la máxima autoridad dentro de esas Instituciones Financieras.

Pregunta N°3. ¿Mencione las funciones principales del Oficial de Riesgo o encargado de la administración del riesgo operacional?

Tabla N° 5: Tabulación de datos resultados de cuestionario, pregunta N°3

RESPUESTAS		
Monitorear	**Evaluar-Clasificar**	**Identificar, medir, controlar y mitigar**
17%	33%	50%

Grafico N°5: Representación gráfica de los resultados de cuestionario, pregunta N°3



Entre todos los encuestados el 50% consideran que las funciones principales se centran en identificar, medir, controlar y mitigar el Riesgo operacional dentro de las instituciones; el 33%

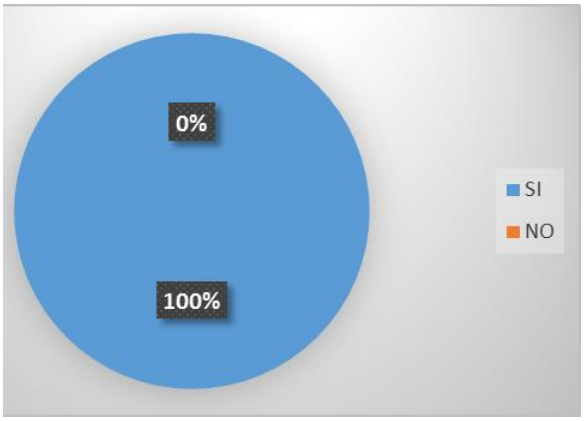
opinan que su función es solamente evaluar y clasificar los eventos de riesgo que se puedan generar y 17% restante consideran que su labor solo es monitorear los eventos de riesgo.

Pregunta N°4. ¿Considera necesario que exista un responsable que se dedique exclusiva o prioritariamente a la gestión de riesgo operacional?

Tabla N° 6: Tabulación de datos resultados de cuestionario, pregunta N°4

Grafico N°6: Representación gráfica de los resultados de cuestionario, pregunta N°4

RESPUESTAS	
SI	NO
100%	0%



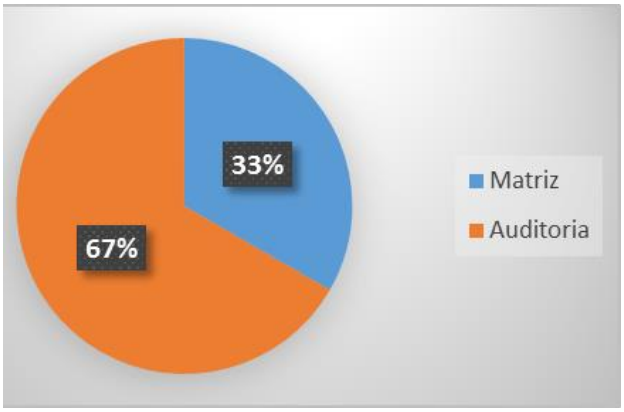
Todas las instituciones encuestadas consideran necesaria la existencia de un responsable del Riesgo operacional, a su vez coindicen en que el riesgo es algo inherente a sus actividades diarias como intermediarias financieras a un sector poblacional que no tiene acceso al sistema financiero tradicional. Por la misma razón opinan que es de gran importancia que contar con alguien permanente en dicha posición.

Pregunta N°5. ¿Cuáles son los métodos de control para riesgo operacional con que cuenta la institución en la actualidad?

Tabla N° 7: Tabulación de datos resultados de cuestionario, pregunta N°5

RESPUESTAS	
Matriz	Auditoria
33%	67%

Grafico N°7: Representación gráfica de los resultados de cuestionario, pregunta N°5



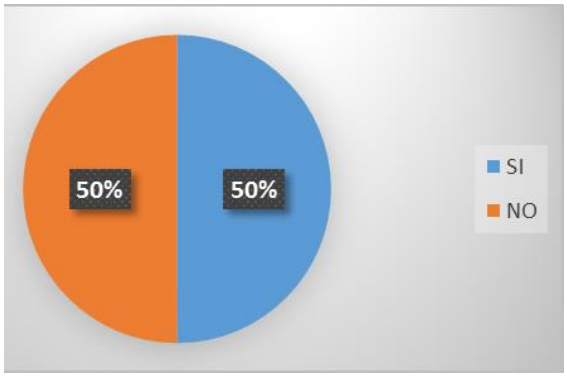
El 67% de los encuestados exponen que se apoyan de Auditorías internas y externas para poder controlar el riesgo Operacional de sus instituciones; por otra parte el 33% mencionan que los encargados de riesgo se basan en matrices de riesgo o tableros de indicadores para poder controlarlo.

Pregunta N°6. ¿Cuentan con una herramienta técnica para identificar, medir, mitigar y controlar riesgos?

Tabla N° 8: Tabulación de datos resultados de cuestionario, pregunta N°6

RESPUESTAS	
SI	NO
50%	50%

Grafico N°8: Representación gráfica de los resultados de cuestionario, pregunta N°6



El 50% de los encuestados han utilizado una matriz de riesgo como herramienta dentro de sus instituciones, pero es de tomar en cuenta que las tres Cajas de Crédito encuestadas coinciden que con la finalidad de efectuar una adecuada administración de riesgos FEDECREDITO les proporcionar una matriz de riesgo operativo como herramienta para el control y gestión que les permite identificar los principales riesgos en relación a los procesos que actualmente ejecutan, por lo que ellos consideran que la están utilizando de manera adecuada.

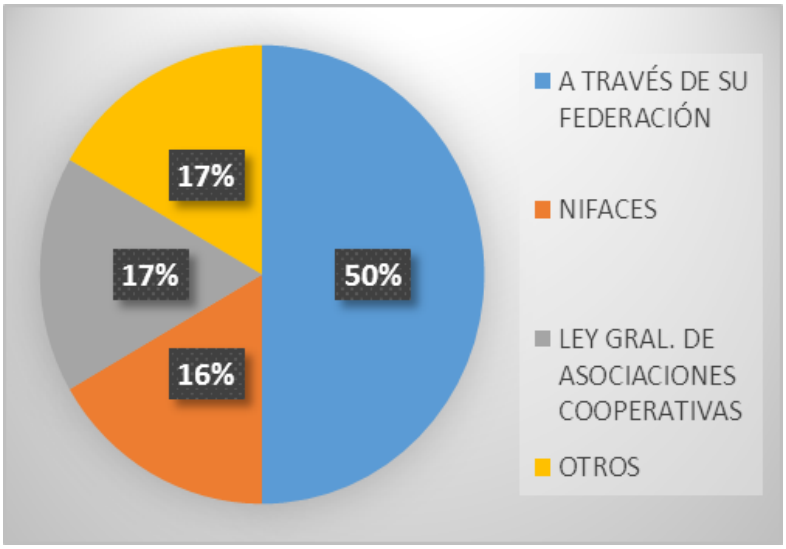
Caso contrario a las otras instituciones encuestadas que no están afiliadas a dicha Federación, comentan que no han utilizado herramientas técnicas específicas para la administración del riesgo operacional y esta ha sido administrada por auditoria o por la persona responsable de dar seguimiento al Riesgo dentro de la institución, pero están conscientes que no son especialistas en esa área por lo que no le sacan el máximo provecho al construirla y analizarla y consideran tienen una oportunidad de mejora al momento de administrarla.

Pregunta N°7. ¿Bajo qué normativas se rige la institución financiera?

Tabla N° 9: Tabulación de datos resultados de cuestionario, pregunta N°7

RESPUESTAS			
A TRAVÉS DE SU FEDERACIÓN	NIFACES	LEY GRAL. DE ASOCIACIONES COOPERATIVAS	OTROS
50%	17%	17%	17%

Grafico N°9: Representación gráfica de los resultados de cuestionario, pregunta N°7



El 50% de los encuestados manifiestan que ellas se rigen por normativas de la Superintendencia del Sistema Financiero de El Salvador, aunque estas instituciones no sean supervisadas directamente por la superintendencia, pero reciben los lineamientos a través de la Federación a la que se encuentra afiliadas, siendo así todas las Cajas de Crédito afiliadas a FEDECREDITO son quienes por manera voluntaria y a través de la Federación, ya están con la normativa de la Superintendencia del Sistema Financiero de El Salvador. El otro 17% expresan que toman en cuenta las normativas del INSAFOCOOP y todas las leyes que competen a El

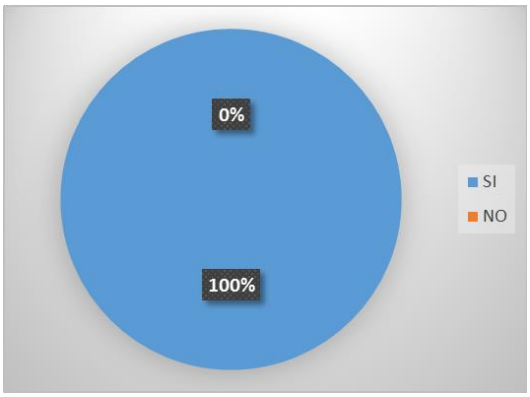
Salvador como son Código de Trabajo, Ley contra lavado de dinero, Defensoría del consumidor, Instructivo de Unidad Financiera, contrato de préstamos contra usura, entre otros. El otro 17% dicen que se rigen por la NIFACES y el restante 17% por la Ley General de Asociaciones Cooperativas.

Pregunta N°8. ¿Considera que los encargados de áreas clave cuentan con el conocimiento debido para mitigar el riesgo operacional dentro de sus áreas?

Tabla N° 10: Tabulación de datos resultados de cuestionario, pregunta N°8

Grafico N°10: Representación gráfica de los resultados de cuestionario, pregunta N°8

RESPUESTAS	
SI	NO
100%	0%



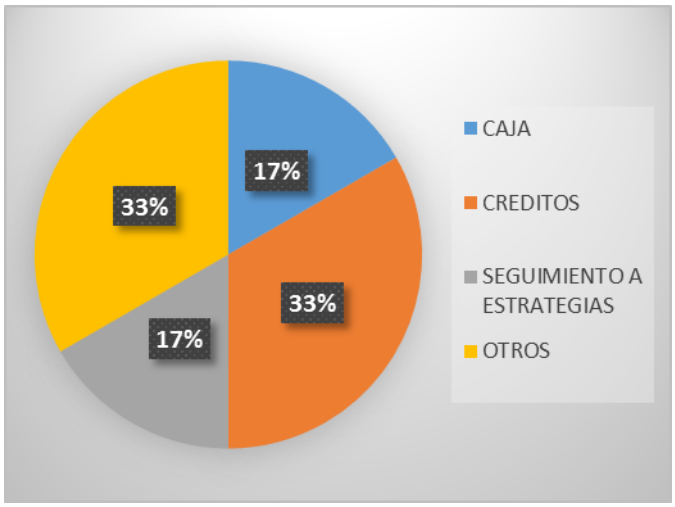
De acuerdo a los datos recolectados en la encuesta mencionan que el 100% consideran que los encargados de áreas claves si cuentan con conocimiento para poder mitigar el Riesgo Operacional dentro de la institución y este lo han adquirido a través de capacitaciones o experiencias anteriores.

Pregunta N°9. ¿Qué procesos considera son los que llevan mayor nivel de riesgo operacional dentro de la institución?

Tabla N° 11: Tabulación de datos resultados de cuestionario, pregunta N°9

RESPUESTAS			
CAJA	CREDITOS	SEGUIMIENTO A ESTRATEGIAS	OTROS
17%	33%	17%	33%

Grafico N°11: Representación gráfica de los resultados de cuestionario, pregunta N°9



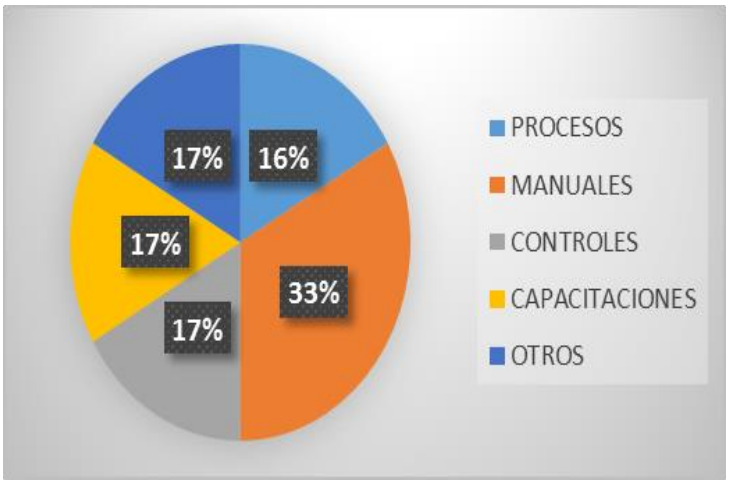
El 33% de los encuestados expresan que el área de Créditos es el proceso que tiene un nivel más alto de riesgo, esto debido a que deben hacer un buen análisis de las personas a quienes les otorgaran los desembolsos. El 17% comenta que el manejo de Caja por el volumen de dinero que manejan y agregado a este el trato directo con el cliente; el otro 17% considera que el tener nuevas estrategias y darle seguimiento a estas le ocasiona el mayor nivel de riesgo. Y en otros tenemos al 33% quienes comentan que todo proceso que involucre varias personas consideran es el que tiene mayor probabilidad de riesgo.

Pregunta N° 10. ¿De qué forma mitigan el riesgo operacional dentro de su institución Financiera?

Tabla N° 12: Tabulación de datos resultados de cuestionario, pregunta N°10

RESPUESTAS				
PROCESOS	MANUALES	CONTROLES	CAPACITACIONES	OTROS
17%	33%	17%	17%	17%

Grafico N°12: Representación gráfica de los resultados de cuestionario, pregunta N°10



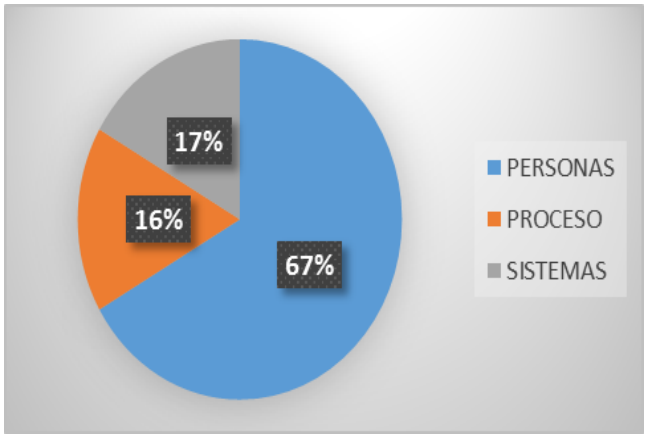
Cada institución encuestada tiene diferentes formas para manejar el riesgo, el 33% indican que es por medio de manuales de procedimientos, el 17% dicen que a través de controles internos, el 17% comentan que por medio de capacitaciones donde dan a conocer la forma para manejar el riesgo y el otro 17% mencionan que cuentan con un comité encargado de mitigar el riesgo, el cual se apoya de las siguientes áreas: Auditoria, área comercial, Oficial de cumplimiento.

Pregunta N°11. ¿Qué factores o áreas considera son los de mayor riesgo operacional dentro de su institución?

Tabla N° 13: Tabulación de datos resultados de cuestionario, pregunta N°11

RESPUESTAS		
PERSONAS	**PROCESO**	**SISTEMAS**
67%	17%	17%

Grafico N°13: Representación gráfica de los resultados de cuestionario, pregunta N°11



El 67% de los encuestados concuerdan que dentro de sus instituciones las personas son el recurso más valioso sin embargo están conscientes que si no los capacitan adecuadamente o no son los perfiles idóneos, pueden convertirse en agentes de mayor riesgo dentro de la misma. El otro 17% considera que son los procesos los que generan riesgo Operacional al no estar definidos de manera adecuada dentro de su institución o no dárseles el seguimiento debido o la supervisión suficiente para asegurarse que los procesos se cumplan, el 17% de los encuestados manifiestan que la mayor fuente de origen del riesgo es el sistema ya que muchas veces no es lo adecuadamente

instruido y lo bastante seguro como por ejemplo con más o mejores controles que garanticen mitigar y controlar el riesgo operacional.

3.1.8 Análisis de la encuesta.

Con los datos recopilados en la encuesta se da respuesta a los objetivos planteados para determinar si las instituciones financieras realmente necesitan un Plan de Mitigación de Riesgo Operacional y si cuentan con un plan de contingencia del negocio.

Basándose en el objeto de estudio, por tratarse de instituciones no Supervisadas por la Superintendencia del Sistema Financiero de El Salvador, las metodologías que utilizan para la identificación, medición, mitigación y control del riesgo, no son las que exige la Superintendencia del Sistema Financiero de El Salvador, siendo ellas mismas de acuerdo al volumen de sus recursos, operaciones, asociados, capital, liquidez, personal, entre otros, quienes establecen de manera interna su propia metodología para contrarrestar la probabilidad de la ocurrencia de los eventos de riesgo, es por ello que este varía por cada institución financiera.

Sin embargo es importante mencionar que las instituciones que están afiliadas a Federaciones reciben lineamientos generales de éstas entre ellos cómo administrar el riesgo, los cuales deben cumplir como requisito para formar parte de ellas.

A pesar de estos lineamientos los resultados obtenidos afirman que en su mayoría las instituciones aún tienen debilidad en los métodos y procesos que utilizan para gestionar el Riesgo Operacional, una de las razones más importantes es que no todas las instituciones cuentan con un Oficial de Riesgo o posiciones similares. Conscientes de ésta debilidad las instituciones intentan apoyarse con otras posiciones como área de auditoria interna, los jefes de agencia, gerente

financiero, comité de riesgo, entre otros, para tratar de controlar ciertos procesos que consideran de mayor riesgo o eventualidades que pudieran generarlos.

Las instituciones encuestadas consideran que dos de las áreas o procesos más vulnerables son los riesgos la inherentes al sector Financiero los cuales están ligados a las operaciones diarias que realizan, como la manipulación de dinero, aprobación y/o recuperación de créditos, desembolsos, etc. y la otra es donde involucra mayor número de personas, como es la atención al cliente, manejo de caja, gestiones de un cheque, el manejo de personal, procesos de cobro, entre otros.

Así mismo con la información recopilada se puede afirmar que las instituciones actualmente no están preparadas para enfrentar un nivel alto de riesgo, ya que ninguna cuenta con un plan de contingencia del negocio que les ayude a identificar los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero sobre la institución.

Por lo que se puede concluir que las instituciones financieras no supervisadas por la Superintendencia Financiera de El Salvador en el Occidente del país, tienen un conocimiento deficiente sobre el manejo de riesgo operacional, por esta razón ponen en riesgo sus operaciones, la cual se considera pueden contrarrestar al elaborar simultáneamente un plan de mitigación para el Riesgo Operacional, así como un plan de continuidad del negocio adecuados al sector en que se desarrollan.

Capitulo IV: Propuesta de un plan de mitigación para el riesgo operacional en instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental.

En el capítulo IV, se presenta la parte más importante del presente trabajo de grado ya que consta de la propuesta de un plan de mitigación para el riesgo operacional en instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental, así como también, se presenta como un complemento de nuestra propuesta, un plan de continuidad del negocio.

4.1 ¿Cómo administrar el riesgo operacional en instituciones financieras no reguladas por la superintendencia del sistema financiero de El Salvador?

El proceso de administración de riesgo operacional, debe permitir a las instituciones identificar, medir, controlar, mitigar y monitorear sus exposiciones a éste riesgo en el desarrollo de sus negocios y operaciones. Cada institución debe desarrollar sus propias técnicas o esquemas de administración, considerando sus características propias, como el objeto social, tamaño, naturaleza, complejidad, recursos, entre otros; además de contar con planes de contingencias y de continuidad del negocio debidamente probado.

Para proceder a identificar áreas críticas en las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador, se deben aplicar cuestionarios de control interno.

Ilustración N°6: Pasos para la administración del riesgo operacional

Elaborado por: Las autoras. Fuente: (Haro, 2003)

4.1.1 PASO 1: Identificación de áreas críticas o factores generadores de riesgo operacional.

4.1.1.1 Procesos.

"Definir y formalizar de manera adecuada sus procesos basado en la planificación estratégica y las políticas establecidas para una mejor identificación de diseño de procesos inadecuados, procesos no documentados o documentación incompleta, implementación inadecuada de procesos, falta de automatización de procesos, ausencia de políticas o políticas inadecuadas, capacidad instalada insuficiente, debilidades en el control interno, debilidades en la seguridad física, contratos inadecuados, selección inadecuada de proveedores, información que carece de sustentación fidedigna." (Palma Rodríguez, 2011)

4.1.1.2 Personas.

Las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador, deben establecer políticas, procesos y procedimientos para una correcta administración del recurso humano, para identificar sus áreas críticas como perfil inadecuado, asignación inadecuada de personal, pérdida del personal clave, negligencia, falta de capacitación y entrenamiento, ausencia de reglamentos internos, proceso de selección de personal inadecuado, accidente de trabajo, enfermedad laboral, actividades no autorizadas, divulgación de información no autorizada.

4.1.1.3 Tecnología de información.

Definir políticas y procedimientos adecuados para una correcta administración de la tecnología de información identificando sus áreas críticas como falta de capacidad de las telecomunicaciones, y hardware, debilidades en la seguridad informática, errores en el diseño de las interfaces, en el diseño de los aplicativos, y en la parametrización de las transacciones, fallas en la asignación de perfiles de usuarios, fallas en el funcionamiento de hardware, mal funcionamiento de software, fallas en redes, y en equipos.

4.1.1.4 Eventos externos.

Eventos que pudieran ocasionar pérdidas financieras derivadas de fallas en los servicios como pueden ser fallas en el suministro de energía, catástrofes naturales, disturbios civiles, actos terroristas, incumplimiento de contratos de terceros, fraude externo, asaltos, robos, negligencia profesional de terceros, cambios en la regulación legales, disposiciones gubernamentales, intrusión en los sistemas informáticos, intrusión en instalaciones físicas.

Las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador deberán elaborar y completar un cuestionario que les permita de obtener una visión general de sus procesos y actividades, que sirva como base para identificar sus propias áreas críticas.

4.1.2 PASO 2: Identificación y evaluación de vulnerabilidades y amenazas.

"Éste paso consiste en identificar las amenazas que pueden afectar a cada activo de la institución. Una amenaza es un agente capaz de explotar accidentalmente o intencionalmente una vulnerabilidad, pero no todas las amenazas afectan a todos los activos; las vulnerabilidades son un defecto o una debilidad en procedimientos sea de seguridad, deficiencia de diseño o implementación de controles internos que podrían ser explotados.

En el siguiente cuadro se identifican las vulnerabilidades y amenazas encontradas en las distintas áreas críticas que arroje el cuestionario de evaluación del control interno de los factores que corresponde el riesgo operacional." (Palma Rodríguez, 2011)

4.1.3 PASO 3: Identificación del riesgo.

La identificación efectiva del riesgo considera tanto los factores internos como externos que podrían afectar adversamente el logro de los objetivos institucionales. Las instituciones deben identificar por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y las fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos.

Ilustración N° 7: Fuentes y eventos de riesgo operacional

FUENTES Y EVENTOS DE RIESGO OPERACIONAL		
RIESGO OPERACIONAL	FUENTES DE RIESGO OPERACIONAL	PROCESOS
		PERSONAS
		TECNOLOGÍA DE INFORMACIÓN
		EVENTOS EXTERNOS
	EVENTOS DE RIESGO OPERACIONAL	FRAUDE INTERNO
		FRAUDE EXTERNO
		RELACIONES Y SEGURIDAD LABORAL
		CLIENTES PRODUCTOS Y PRACTICAS
		COMERCIALES
		DAÑOS O PERDIDAS DE ACTIVOS
		INTERRUPCION DEL NEGOCIO
		INTERRUPCION DEL SISTEMA DE EJECUCION
		ENTREGA Y GESTIÓN DE PROCESOS

Elaborados por: Los autores. Fuente: (Gumercindo Ruíz, 2000).

Cada uno de los eventos de riesgo operativo así como sus deficiencias se identifican en relación con los cuatro pilares que comprende el riesgo operacional utilizando una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, matriz de riesgo, indicadores, tablas de control, bases de datos u otras; las instituciones deben determinar las fallas o insuficiencias, de manera que tengan una visualización sobre su exposición al riesgo, las mismas deben ser establecidas de acuerdo con su propio conocimiento y perfil de riesgos, pero deben estar orientadas al menos a los siguientes campos: actos societarios; gestión de crédito; operaciones del giro financiero; actividades complementarias no financieras; y, cumplimiento legal y normativo. En la siguiente tabla se especificará, para cada factor de riesgo descrito en la anterior tabla, distribuido de acuerdo a su área el origen del riesgo; así como su potencial consecuencia.

4.1.4 PASO 4: Determinación de la probabilidad de ocurrencia y grado de impacto potencial.

"Para todos los riesgos operacionales materiales que se identifiquen, las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador, deben decidir si usa procedimientos apropiados de control y mitigación de los riesgos o asumirlos para los que no pueden ser controlados, también deben decidir si los aceptan, mitigar, trasladar o eliminar la actividad que origina dicho riesgo. Cada institución debe contar con estrategias de mitigación, como los seguros. Cada uno de los riesgos materiales debe ser evaluado mediante la probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de las instituciones a éste riesgo. Se trata de un método práctico para determinar qué tan probable es que se dé una eventualidad que afecte a las instituciones. Se realizará un análisis de los factores de riesgo, de acuerdo a la ubicación que le corresponda en el mapa de riesgo que deberá considerar las siguientes características:

Se valorarán tanto la Probabilidad de Ocurrencia del suceso de riesgo y el Grado de Impacto Potencial del mismo sobre la operación de las instituciones, para determinar el Nivel de Riesgo o Gravedad del Factor o Suceso de Riesgo." (Madinya, 2013)

4.1.4.1 Determinación de la probabilidad de ocurrencia.

"En el eje horizontal se ingresará la valoración de la PROBABILIDAD DE OCURRENCIA del suceso de riesgo, entre un rango del 1 al 3, siendo 1 una baja probabilidad de ocurrencia y 3 una alta probabilidad de ocurrencia del suceso.

Ilustración N°8: Determinación de la probabilidad de ocurrencia del factor de riesgo

DETERMINACIÓN DE LA PROBALIDAD DE OCURRENCIA DEL FACTOR DE RIESGO			
PUNTUACIÓN	**CLASIFICACIÓN**	**PARÁMETRO DE PROBABILIDAD**	**FRECUENCIA DEL SUCESO DE RIESGO**
1	**BAJA**	Podría ocurrir sólo en circunstancias excepcionales.	Una vez cada 10 años o menos frecuente.
2	**MEDIA**	Podría ocurrir alguna vez.	Una vez cada 3 o 5 años.
3	**ALTA**	Ocurriará alguna vez.	Una vez cada año o mensualmente.

Elaborado por: Las autoras. Fuente: (Madinya, 2013)

4.1.4.2 Determinación del grado de impacto.

En el eje vertical se ingresará la valoración del GRADO DE IMPACTO POTENCIAL que se considera que tiene el suceso de riesgo, el cual será entre un rango del 1 al 3, en donde 1 representa un bajo grado severidad sobre el resultado del proceso y 3 una severidad tal que interrumpe completamente las operaciones de la institución.” (Madinya, 2013)

Ilustración N°9: Determinación de grado de impacto potencial de factor de riesgo

DETERMINACIÓN DEL GRADO DE IMPACTO POTENCIAL DEL FACTOR DE RIESGO			
PUNTUACIÓN	**CLASIFICACIÓN**	**PARÁMETRO DE IMPACTO**	**EXPOSICIÓN MEDIATICA DEL SUCESO**
1	**BAJO**	No impacta a los clientes	No hay divulgación de problemas ni propaganda del suceso.
2	**MEDIO**	Repercusiones sobre los clientes	Artículos en prensa, televisión, internet, es decir divulgación significativa por mas de un día.
3	**ALTO**	Suspensión prolongada del servicios	Repercusiones gubernamentales a nivel político y pérdida de confianza del público.

Elaborado por: Las autoras. Fuente: (Madinya, 2013)

4.1.5 PASO 5: Medición o valoración de la gravedad del riesgo.

"En éste paso se utiliza una tabla llamada Mapa de Riesgo para valorizar el nivel del riesgo, en función de probabilidad de ocurrencia e grado de impacto potencial el mismo que es resultado de la combinación probabilidad e impacto, es decir que se combinan así: si al impacto se calificó como ALTO = 3 y la probabilidad igualmente ALTA = 3, entonces tenemos el nivel de riesgo 3 x 3 = 9 que significa que el riesgo es INMENENTE. Tal como lo observamos en el mapa, definimos si se trata de un riesgo MÍNIMO valor 1 y el color que observamos, o un riesgo valorado como MODERADO de 3 a 4, bueno entre el nivel uno y nueve hay una gama de colores permitiéndonos tener una visión rápida de la magnitud del riesgo por el propio color." (Madinya, 2013)

Ilustración N° 10: Medición o valorización del riesgo

MEDICIÓN O VALORIZACIÓN DEL RIESGO					
MAPA DE RIESGO			PROBABILIDAD DE OCURRENCIA DEL SUCESO DE RIESGO		
			BAJA	MEDIA	ALTA
			1	2	3
GRADO DE IMPACTO POTENCIAL DEL SUCESO DE RIESGO	ALTO	3	3 (MODERADO)	6 (ALTO)	9 (INMINENTE)
	MEDIO	2	2 (BAJO	4 (MODERADO)	6 (ALTO)
	BAJO	1	1 (MINIMO)	2 (BAJO)	3 (MODERADO)

Elaborado por: Las autoras. Fuente: (Madinya, 2013)

4.1.6 PASO 6: Clasificación y determinación de la gravedad del riesgo.

Una vez determinada la probabilidad de ocurrencia del riego y el grado del impacto de cada factor de riesgo, se debe clasificar y determinar el nivel o gravedad del riesgo, que es el resultado de la combinación de estas dos variables, NIVEL O GRAVEDAD DE RIESGO: (PROBALIDAD)*(IMPACTO).

Luego se dará respuesta al riesgo, la cual podría ser: EVITAR, REDUCIR, ACEPTAR; para posteriormente analizar los controles con los que cuentan las instituciones, es decir determinar cuál es su Efectividad de los Controles o Grado de Exposición al Riesgo, resultado que servirá

para calcular el Riesgo Residual para proponer medidas correctivas. El riesgo de acuerdo a su localidad en el mapa, presentan diferentes grados de prioridad de respuesta en la gestión.

Ilustración N°11: Nivel de riesgo conforme a la zona de ubicación del suceso en el mapa de riesgo

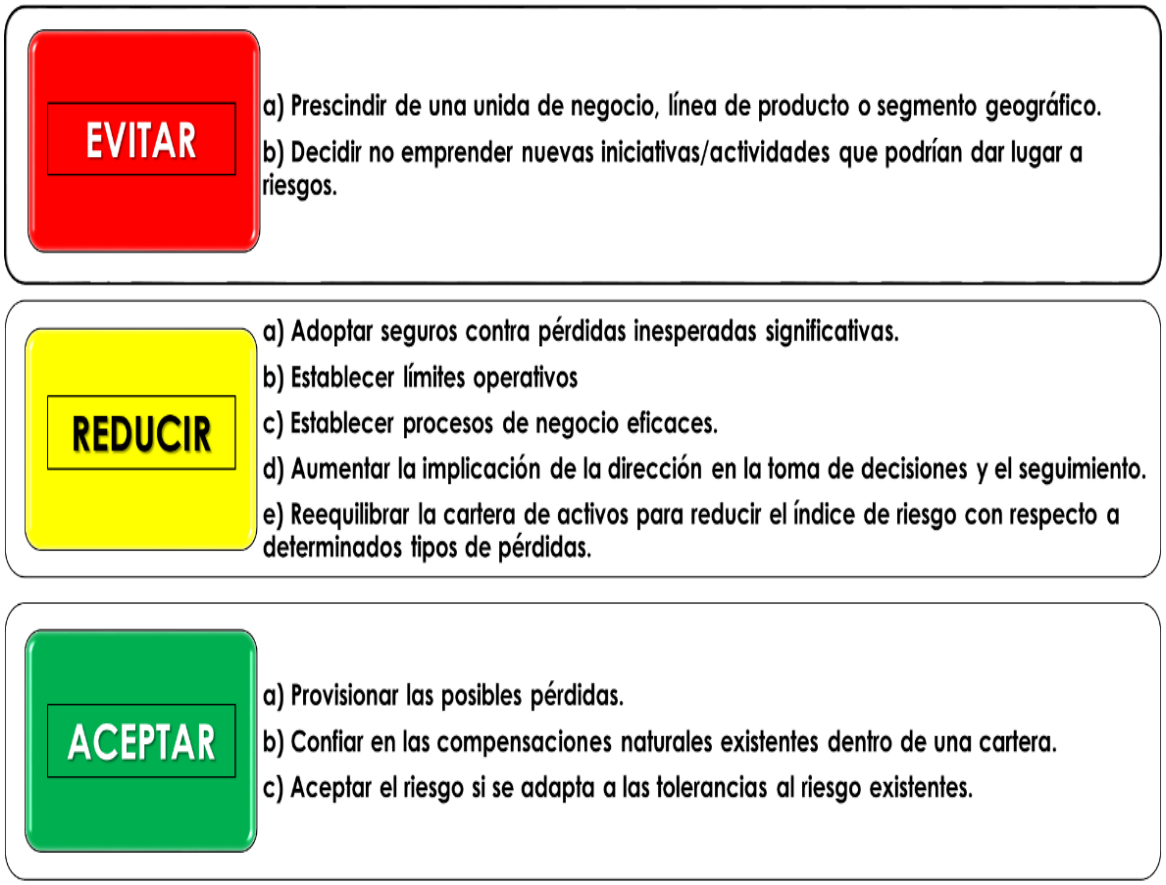
NIVEL DE RIESGO CONFORME A LA ZONA DE UBICACIÓN DEL SUCESO EN EL MAPA DE RIESGO				
UBICACIÓN EN EL MAPA	**NIVEL DE RIESGO DEL SUCESO**	**RESPUESTA ANTE EL NIVEL DE RIESGO DEL SUCESO**	**SIGNIFICADO DEL NIVEL DE RIESGO**	**NIVEL DE PRIORIDAD**
ROJO	**ALTO / INTOLERANTE**	El Riesgo debe ser: **EVITADO**	Afecta a gran parte de la institución o a toda la institución.	**1**
AMARILLO	**MEDIO / TOLERANTE**	El Riesgo debe ser: **REDUCIDO**	Afecta al trabajo de otros y/o a todo un proceso.	**2**
VERDE	**BAJO / ACEPTABLE**	El Riesgo puede ser: **ACEPTADO**	Facil de superar y corregir.	**3**

Elaborado por: Las autoras. Fuente: (Palma Rodríguez, 2011).

4.1.7 PASO 7: Respuesta al riesgo.

Una vez que se ha determinado los riesgos relevantes, las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador, deben determinar cómo responder a ellos. Las respuestas pueden ser la de evitar, reducir o aceptar el riesgo. Al considerar la respuesta deben evaluar su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios.

Ilustración N° 12: Semáforo de respuesta ante el riesgo operacional



Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012)

4.1.8 PASO 8: Evaluación de la calidad de la gestión o exposición al riesgo.

Una vez valorizados los riesgos se procede a evaluar la calidad de la gestión del riesgo, es decir la efectividad de los controles por parte de la institución para mitigar los riesgos identificados. La exposición al riesgo se determina en base a qué tanto le afecta a la institución el riesgo ya que se mantiene cierta posición y por lo tanto es vulnerable a lo que pueda suceder, es decir está expuesta. Es importante aclarar que el grado de exposición es inverso a la efectividad de los controles y mitigantes que se mantienen ante un determinado riesgo, es decir entre más controles

tenga sobre un riesgo, disminuye la exposición a sufrir una pérdida.: **EXPOSICIÓN = RIESGO - CONTROL.**

Una vez valorizados los riesgos se procede a evaluar la "calidad de la gestión" a fin de determinar cuán eficaces son los controles establecidos por la institución para mitigar los riesgos identificados.

Ilustración N°13: Determinación del grado de exposición al riesgo de acuerdo a la efectividad de los controles.

DETERMINACIÓN DE GRADO DE EXPOSICIÓN AL RIESGO DE ACUERDO A LA EFECTIVIDAD DE LOS CONTROLES				
PUNTUACIÓN	**CLASIFICACIÓN**	**EXISTENCIA DE PROCEDIMIENTOS**	**CONTROLES**	**PLANES DE MITIGACIÓN DE RIESGOS**
1	**BAJA**	Procedimientos exhaustivos para cada situación y actualizados diariamente.	Roles claros y detallados, controles automáticos y preventivos, responsabilidades bien definidas.	Al materializase el riesgo el trabajo puede continuar porque existe un tercero al cual se transmitirá el riesgo y existe un plan de contingencia.
2	**MEDIA**	Procedimientos para áreas claves, actualizaciones periodicas.	La mayoria de roles definidos, algunos controles automáticos o manuales y algunos controles preventivos.	El riesgo ha sido parcialmente transferido a un tercero.
3	**ALTA**	Procedimientos mínimos o nulos, ausencia de actualizaciones.	No existe definición de roles, controles, ni responsabilidades.	No existe plan de contingencia, es decir el riesgo no se ha transferido a un tercero.

Elaborado por: Las autoras. Fuente: (Palma Rodríguez, 2011)

La matriz de riesgo relaciona el nivel de riesgo de la entidad financiera, con la exposición anticipada del riesgo. Considerando variables cualitativas (características del recurso humano, procesos, tecnologías y eventos externos) y las transformamos en variables cuantitativas para conocer el riesgo, cuantificarlo, monitorearlo y mitigar o eliminar el riesgo operativo.

Una vez determinados el nivel de riesgo y el grado de exposición al mismo, podemos llegar a elaborar una Matriz de Riesgo:

Ilustración N°14: Matriz de riesgo

MATRÍZ DE RIESGO			NIVEL DE RIESGO		
			BAJO	MEDIO	ALTO
			1	2-4	6-9
GRADO DE EXPOSICIÓN AL SUCESO DE RIESGO	ALTA	3	B	C	C
	MEDIA	2	B	B	C
	BAJA	1	A	B	B

Elaborado por: Las autoras. Fuente: (Palma Rodríguez, 2011)

En la parte vertical medimos la puntuación de los parámetros de exposición y horizontalmente encontraremos el nivel de riesgo de la entidad, agrupados en intervalos de valores.

Ilustración N°15: Evaluación de la calidad de la gestión del riesgo

EVALUACIÓN DE LA CALIDAD DE LA GESTIÓN DEL RIESGO	
CALIFICACIÓN DE LAS ÁREAS CRÍTICAS	**INTERPRETACIÓN DE LA CALIFICACIÓN DE RIESGO**
A	Nos indica que se tiene identificado y cuantificado el riesgo operativo, así como la forma de mitigación del riesgo operativo.
B	Nos indica situaciones intermedias o concentradas en una variable ya sea de exposición o riesgo, que ameriten elaborar medidas de mitigación del riesgo operativo.
C	Representa una situación crítica e irregular de la entidad con mucha exposición y niveles altos de riesgos que se deben de atender en forma inmediata.

Elaborado por: Las autoras. Fuente: (Palma Rodríguez, 2011)

4.1.9 PASO 9: Plan de mitigación de riesgo operacional.

Mitigar el riesgo significa reducir la probabilidad y/o el impacto de alguna situación de riesgo contrario a lo permitido o aceptado, aunque más efectivos es optar por medidas tempranas para educir la probabilidad de la ocurrencia de un riesgo y/o su impacto antes que tratar de reparar el daño después de que ha ocurrido el riesgo. Luego de determinar la probabilidad por el impacto para cada factor de riesgo, se analiza la efectividad de los controles con los que cuenta la institución y se valoriza los mismos, para hacer frente con el riesgo existente de cada factor, dando como resultado el riesgo residual; una vez determinado el riesgo residual de cada factor de riesgo se analiza cada uno con el objetivo de dar medidas o recomendaciones, así como también de conocer cuál es la prioridad de que dichas medidas se materialicen, en que tiempo y sus respectivos indicadores.

4.2 ¿Cómo construir un plan de mitigación para el riesgo operacional para instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador?

Ilustración N° 16: Pasos para desarrollar un plan de mitigación para el riesgo operacional

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012)

4.2.1 PASO #1: Evaluación de control interno.

Para evaluar su control interno, las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador, deberán elaborar y responderse un cuestionario que esté enfocado en los procesos, las personas, la tecnología de información y los eventos externos, con el fin de identificar la eficiencia de sus controles y las vulnerabilidades con las que opera la institución.

4.2.1.1 Generales.

Tabla N° 14. Cuestionario de evaluación de control interno para generalidades

ÁREA OPERATIVA: PREGUNTAS GENERALES			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿La institución cuenta con una estructura organizacinal definida?	X	
2	¿Dentro de esta estructura organizacional existen niveles jerárquicos Gerencia General, Vicepresidentes ejecutivos, Gerentes departamentales responsables de ejecutar las disposiciones de la Junta o Asamblea General?	X	
3	¿La institución cuenta con un proceso de administración de la información en la cual se captura, procesa, almacen a y trasmite información, independiente del medio que se utilice; sea impreso, escrito en papel, almacenado electrónicamente, trasmitido por correo o por medios electrónicos o presentado en imágenes?	X	
4	¿La institución cuenta con infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información?	X	
5	¿La institución cuenta con procedimientos alternativos a la operatividad normal cuya finalidad es la de permitir su funcionamiento,en cualquier evento inesperado?	X	
6	¿La institución tiene establecido esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio?		X
7	¿Cuenta la institución con un Comité de administración integral de riesgos, que es el órgano creado por el directorio u organismo que haga sus veces de la institución del sistema nanciero, el mismo que es responsable del diseño de las políticas, sistemas, metodologías, modelos y procedimientos, para la eficiente gestión integral de los riesgos y de manera específica en los identificados en la actividad que efectúa la institución?		X
8	¿la institución cuenta con una Unidad de administración integral de riesgos que es un órgano autónomo responsable de identificar,medir, monitorear, controlar, mitigar y divulgar cada uno de los riesgos identificados que enfrenta la institución del sistema financiero y su concordancia con las políticas que al efecto han sido emitidas por ella?		X
9	¿Existe un control de entrada y salida de información para que la misma sea confiable?	X	
10	¿Los procesos están totalmente automatizados?		X
11	¿Cuenta la institución con un plan de contingencia, para contrarrestar deficiencias en los procesos?		X

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.1.2 Procesos.

Tabla N°15. Cuestionario de evaluación de control interno para áreas de Procesos

ÁREA OPERATIVA: PROCESOS			
VERIFICACIÓN DE LA IDENTIDAD			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿Recibe a las personas que se presentan manifestando el deseo de realizar una operación financiera a través del sistema?	X	
2	¿Solicita los detalles de la operación?	X	
3	¿Solicita cédula de idinstitución o documentación que permita verificar la idinstitución del solicitante?	X	
4	¿Verifica que los datos incluidos en la documentación presentada sean coincidentes con la persona y con la información que ésta provea?	X	
5	¿Si existen dudas con respecto a la veracidad de la documentación presentada, se solicita complementación de la documentación presentada con Libreta de Aportaciones o documentación personal que acrediten su idinstitución?		X
6	¿Si luego del análisis de la documentación adicional la idinstitución verificarse con certeza, se envía Gerencia para su revisión?	X	
7	¿Si no existen dudas sobre la idinstitución de la persona se ingresa al módulo de Operaciones Financieras del sistema e ingresa los datos de la misma a fin de obtener el listado de cuentas?	X	

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°16. Cuestionario de evaluación de control interno para áreas de Procesos de caja.

ÁREA OPERATIVA: PROCESOS			
CAJA			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿Existe procedimientos escritos del uso de la caja?		X
2	¿Existen formatos para reportes de caja?	X	
3	¿Se realizan arqueos de caja sorpresivos del fondo de caja?		X
4	¿Cada cajero prepara y firma el reporte de cuadre de caja diario detallado el efectivo en su caja, de acuerdo a la cantidad de billetes y monedas?	X	
5	¿El efectivo de cada caja es conciliado diariamente con el sistema?	X	
6	¿Las diferencias encontradas son reportadas y revisadas por un superior?	X	
7	¿Las transferencias de dinero entre cajeros son supervisadas y autorizadas?	X	
8	¿Se limita a los cajeros que puedan laborar en otros departamentos?	X	
9	¿El cajero verifica minuciosamente los documentos, firmas de los socios?		X
10	¿Existen un control restringido sobre las llaves de las cajas?		X

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°17 Cuestionario de evaluación de control interno para áreas de Procesos de pagos.

ÁREA OPERATIVA: PROCESOS			
PAGOS			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿Selecciona, entre las opciones mostradas por el sistema, la cuenta de ahorro indicada por el cooperativista o socio y consulta los datos generales de la misma?	X	
2	¿Verifica que el cooperativista o socio sea titular de una cuenta activa, requiriéndole su cédula de idinstitución, su libreta de ahorros?	X	
3	¿Efectúa el control de firmas en el caso que no se presente personalmente el cooperativista titular, se requerirá al presentante la correspondiente autorización escrita firmada por aquél y se verifica la coincidencia de ésta con la que brinda el sistema?	X	
4	¿De no contar con la imagen de la firma, se comprueba a través de fax enviado por la institución donde está radicada la cuenta?	X	
5	¿Si no es posible comprobar la titularidad de la cuenta o ésta no se encuentre activa, se informa a quien pretende efectuar el retiro que no es posible procesar dicha operación?	X	
6	¿De lo contrario, se ingresa el tipo de operación "Retiro de Ahorros", el monto indicado por el cooperativista y la forma de pago, y se procesa la operación?	X	
7	¿Si no existen dudas sobre la institución de la persona se ingresa al módulo de Operaciones Financieras del sistema e ingresa los datos de la misma a fin de obtener el listado de cuentas?		X
8	¿El sistema valida que la cuenta disponga de saldo suficiente para realizar la operación, si el sistem a rechaza la operación, se informa al cooperativista o socio que su saldo no es suficiente y que puede intentar retirar un monto menor?		X
9	¿Si la operación es aprobada, en forma automática se dispondrá para imprimir el comprobante de la operación?		X
10	¿Realiza impresiones del comprobante de la operación?	X	
11	¿Solicita la firma del cooperativista sobre 2 copias de los comprobantes impresos, archiva uno en la documentación de caja y el restante se archiva como documentación de control?		X
12	¿Sella la copia restante y entrega al solicitante junto con el dinero?		X

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012)

Tabla N°18. Cuestionario de evaluación de control interno para áreas de Procesos de recaudación.

ÁREA OPERATIVA: PROCESOS			
RECAUDACION			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿Existen políticas y manuales de recuperación de cartera vencida?	X	
2	¿Existe un monitoreo diario de la cartera en mora?	X	
3	¿Existe una buena coordinación entre el departament o de cobros y gerencia para disminuir los índices de morosidad?	X	
4	¿Existe un reporte en el sistema que detalle el comportamiento de la cartera?	X	
5	¿Se lleva un control de visita de cobros realizada a los socios con saldo en mora?	X	
6	¿Hay un procedimiento para la depuración de carter a morosa?		X
7	¿Existe políticas para el proceso de recaudación?		X
8	¿Selecciona, entre las opciones mostradas por el sistema, la cuenta de ahorro o oportaciones ordinarias indicada por el cooperativista y consulta los datos generales de la misma?	X	
9	¿Si el monto del depósito contiene alguna de las características indicadas en el párrafo anterior, onfecciona formulario de declaración de licitud de fondos y transacciones y solicita al depositante lo complete en las partes pertinentes y lo firme?	X	
10	¿Si la persona no completa y firma el formulario indicado, deja sin efecto la operación, reintegrándole documentación, de lo contrario, continúa con los pasos siguientes?	X	
11	¿Ingresaeltipodeoperación"Depósito de Ahorro"/"Depósito de Aportaciones" y el monto indicado por el cooperativista?	X	
12	¿Para imprimir el comprobante de la operación dispo ne en forma automática?		X

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°19. Cuestionario de evaluación de control interno para áreas de Procesos de pagos de servicios.

ÁREA OPERATIVA: PROCESOS			
PAGO DE SERVICIOS BÁSICOS			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿Existe un manual de procesos para el pago servicios básicos?		X
2	¿Solicita el número o código al socio?		X
3	¿Escoge entre las opciones mostradas por el sistema, la opción requerida por el cliente?	X	
4	¿Ingresa el número al sistema?	X	
5	¿El sistema indica el monto a pagar?	X	
6	¿Informa al socio o cliente el valor?		X
7	¿Cobra el valor, e ingresa al sistema para impresión de documento?		X
8	¿Imprime el documento y entrega al socio o cliente?	X	
9	¿Automáticamente se envía la información a la central de cobros?	X	

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.1.3 Personas.

Tabla N°20. Cuestionario de evaluación de control interno para áreas de Personas

ÁREA OPERATIVA: PERSONAS			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	¿Existe un manual de procesos de incorporación del nuevo personal?		X
2	Cuál de los siguientes procesos se toma en cuenta en el manual de incorporación del personal:		
3	Planificación de necesidades	X	
4	Reclutamiento	X	
5	Selección	X	
6	Contratación e inducción.	X	
7	¿Existe un manual de procesos de permanencia del personal?		X
8	En el manual del proceso de permanencia consta de:	X	
9	¿Capacitación y formación del personal?		X
10	¿Un sistema de evaluación de desempeño?	X	
11	¿Rendición de cuentas?		X
12	¿Reconocimiento al personal por su desempeño?		X
13	¿Un proceso de rotación de personal?	X	
14	¿Un proceso de seguimiento para determinar el cumplimiento de las funciones asignadas al personal?	X	
15	¿Existe un reglamento interno para el personal?		X
16	¿Cuenta con un seguro para accidentes de trabajo?		X
17	¿Existe un manual de procesos de desvinculación del personal?		X
18	¿Para la desvinculación del personal existe una planificación de la salida del mismo por causas regulares?	X	
19	¿Para los procesos de desvinculación se hace por me dio del organismo competente?		X
20	¿La institución mantiene actualizada información del capital Humano para una adecuada toma de decisiones?		X
21	¿Cuenta la institución con un Código de Ética?	X	
22	¿Existe una adecuada segregación de funciones?	X	

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.1.4 Tecnología de información.

Tabla N°21. Cuestionario de evaluación de control interno para áreas de Tecnología de información.

ÁREA OPERATIVA: TECNOLOGÍA DE INFORMACIÓN			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	Con el objeto de garantizar que la administración de la Tecnología de Información soporte adecuadamente los requerimientos de la institución, la institución cuenta con:		
2	¿Apoyo de la Gerencia y Directorio?	X	
3	¿Un plan funcional de TI alineado con plan estratégico de la institución?		X
4	¿Un responsable de la información que se encargue de los accesos, cambios funcionales a las aplicaciones, monitoreo de controles?	X	
5	¿Difusión y comunicación de políticas, procesos y procedimientos al personal involucrado para asegurar su implementación?	X	
6	Con el objeto de garantizar que las operaciones de TI satisfagan los requerimientos de la institución la institución cuenta con:	X	
7	Manuales o reglamentos internos aprobados por el directorio que establezcan:		
8	Responsabilidades y procedimientos para la operación	X	
9	¿Uso de las instalaciones de procesamiento de la información?	X	
10	¿Respuestas a incidentes de TI?		X
11	Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades y estén sometidas a un monitoreo, la institución cuenta con:		
12	¿Responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas?		X
13	¿Transferencia del conocimiento por parte del proveedor?		X
14	¿Entrega documentación técnica y de usuario?		X
15	Con el objeto de garantizar que el sistema de administracióndeseguridadsatisfagalas necesidades de la institución para salvaguardar la información contra el uso, modificación no autorizados, daños y pérdidas, la institución cuenta con:		X
16	¿Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, y responsabilidades?	X	
17	¿La identificación de los requerimientos de seguridad relacionados con la tecnología de información?	X	
18	¿Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada?	X	
19	¿Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría?	X	
20	¿Niveles de autorización de accesos que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude?		X

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.1.5 Eventos externos.

Tabla N°22. Cuestionario de evaluación de control interno para áreas de Eventos Externos

ÁREA OPERATIVA: EVENTOS EXTERNOS			
N°	**PREGUNTAS**	**RESPUESTA**	
		SI	**NO**
1	La institución cuenta con planes de contingencia y de continuidad del negocio, en caso de que ocurra algún evento ajeno a su control como:		
2	¿Fallas en el suministro de energía?		X
3	¿Catástrofes naturales?		X
4	¿Disturbios civiles?		X
5	¿Actos terroristas?		X
6	¿Incumplimiento de contratos de terceros?		X
7	¿Fraude externo/ Asalto/ Robo?		X

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012)

4.2.2 PASO #2: Identificación de los factores de riesgos.

Luego de evaluar el control interno de la institución, se debe analizar para identificar los factores generadores de riesgo. Se debe separar por áreas, para que en cada una se puedan determinar los objetivos o actividades y el proceso, así como el responsable, para finalmente, especificar los factores generadores de riesgo inherentes a cada actividad desarrollada por las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador.

4.2.2.1 Generales.

Tabla N°23. Cuestionario de identificación de los factores de riesgo para áreas generales

ÁREA OPERATIVA: GENERALES				
ACTIVIDADES	**PRODUCTOS**	**PROCESO**	**RESPONSABLE**	**FACTOR DE RIESGO**
Definir la estructura orgánica de acuerdo a los objetivos de la institucion.	Organigrama	1. Autorización y apoyo de los niveles superiores. 2. Acopio de la información. 3. Clasificación y registro de la información.	Gerencia. Concejo de Administración	No se actualice la estructura orgánica.
	Niveles Jerárquicos definidos	4. Análisis de la información. 5. Diseño del organigrama de acuerdo a los cargos y esponsabilidades. 6. Socializar las responsabilidades.	Gerencia. Concejo de Administración	Desconocimiento de los cargos por parte del personal de la institución
Definir un proceso de administración de la Información	Información procesada, almacenada y trasmitida.	1. Clasificación de la información. 2. Ingreso para procesamiento de la información. 3. Almacenamiento de la información 4. Difusión de la información.	Gerencia. Concejo de Administración.	Errores en el ingreso de la información. Espacio de almacenamiento insuficiente. Que la información difundida sea incorrecta.
Construir infraestructura que permita alojar recursos físicos relacionados con TI.	Infraestructura construida	1. Análisis del Volumen de las operaciones de la institución. 2. Contratación de personal para la construcción de la infraestructura. 3. Adquisición de materia prima necesaria para la obra. 4. Construcción de la infraestructura.	Gerencia. Concejo de Administración.	Falte espacio físico. Disponibilidad de información y documentación confidencial. Disponibilidad al polvo. No apoyar la continuidad de operaciones. Mayor deterioro del Equipos.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.2.2 Proceso.

Tabla N°24. Cuestionario de identificación de los factores de riesgo para áreas de Procesos.

ÁREA OPERATIVA: PROCESOS				
ACTIVIDADES	**PRODUCTOS**	**PROCESO**	**RESPONSABLE**	**FACTOR DE RIESGO**
Verificación de idinstitución	Identificación de los datos de la persona	1. Recibe a las personas que van a realizar una operación financiera. 2. Solicita detalles de la operación y documentación 3. Verifica los mismos, que sean coincidentes con la persona. 4. Si es así proceden a realizar la petición del socio o cliente 5. De lo contrario será negativa la operación.	Cajero	Que no se verifique minuciosamente los documentos y firmas de los socios.
Caja	Arqueo de caja	1. Se realizan arqueos de caja diariamente por cada cajero. 2. Los mismos deben cuadrar. 3. Estar detallados y de acuerdo a la cantidad de billetes y monedas. 4. Deben conciliarse con el sistema. 5. Existe un control restringido sobre las llaves de las cajas.	Cajero	No se realicen arqueos oportunos de caja. Robo de dinero y documentos mercantiles.
Pagos	Pago del dinero con respectivo recibo	1. Se selecciona en el sistema la opción requerida por el socio. 2. Se verifica que sea titular de una cuenta requiriéndole su cédula de idinstitución. 3. A la misma que se realiza un control de firmas. 4. En caso de no presentarse el titular se requerirá al representante la autorización por escrito y firmada por aquél. 5. De ser positiva la idinstitución y firma, se ingresa los datos al sistema. 6. Automáticamente se dispondrá el estado de cuenta, mediante el cual se aprobará o negará el requerimiento del socio. 7. Si es aprobatorio de forma automática se dispondrá para imprimir el comprobante de la operación 8. Y por último se sella la copia y entrega al solicitante junto con el dinero.	Cajero	No contar con su respectiva documentación para el sustento del socio/cliente como para la institución. Que no se emitan comprobantes de las transacciones realizadas. No tener el respaldo de la persona de que hizo la transacción tanto de la institución como el beneficiario.
Recaudación	Recuperación de cartera en mora, Recaudación de depósitos	1. Selecciona entre las opciones mostradas por el sistema, la cuenta de ahorros indicada por el socio. 2. Verifica el monto del depósito a efectuar, si el mismo es igual o mayor al indicado, o si contiene alguna de las características establecidas en la "Ley de Lavado d e Activos". 3. Llena formulario de declaración de licitud de	Cajero/ra. Oficial de crédito. Gerencia	Que el origen de los fondos no sea lícito; Que existan billetes falsos.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°25. Cuestionario de identificación de los factores de riesgo para áreas de Procesos.

ÁREA OPERATIVA: PROCESOS				
ACTIVIDADES	**PRODUCTOS**	**PROCESO**	**RESPONSABLE**	**FACTOR DE RIESGO**
Cobrar consumo de servicios básicos	Cobro de servicios básicos	1. Se solicita el número o código al socio o cliente. 2. Escoge entre las opciones mostradas por el sistema la requerida por el socio/cliente. 3. Ingresa el numero/código al sistema. 4. El sistema indica el monto a pagar, el mismo que es informado al socio. 5. Cobra el valor o monto por el servicio e ingresa al sistema para impresión del comprobante. 6. Imprime el documento y entrega al socio o cliente.	Cajero	Cobrar servicio de un usuario diferente.
Créditos	Créditos de consumo, hipotecarios e inversión	1. Al momento de la atención al socio del crédito, se piden referencias básicas como: Cuál será inversión del crédito, información de actividad, ingresos, gastos, e informan sobre las políticas de crédito etc. 2. Previa a la calificación del socio se verifica en central de riesgos la misma. 3. En la entrega se solicitud y requisitos para crédito los mismos son de acuerdo al tipo de crédito 4. El análisis socioeconómico del socio, se realiza mismo que se realiza las 5"C". 5. Para dar seguimiento del crédito, en coordinación con gerencia, se realiza un muestreo y visitas sin previo aviso. 6. Cuando un cliente se encuentra en mora, se puede cubrir dicho valor con recursos de garantes, previo aviso al mismo. 7. Por último se archiva la documentación por número de créditos en carpeta independiente.	Analista de créditos	Crédito otorgado sin el análisis respectivo. No se cuente con niveles de aprobación del otorgamiento del crédito. No pedir referencias suficientes al socio sobre cuál será el destino del crédito. No se verifique la calificación del socio en la Central de Riesgos. Para el estudio socioeconómico del debitar de los saldos disponibles de la socio no se analice las cinco "C". Cuando se proceda a la recuperación administrativa no exista políticas para cuenta de ahorros de los socios No se cubra el valor en mora del cliente con recursos del garante.
Compras	Adquisición de bienes, Software y Hardware.	1. La institución determina los requerimientos de compras 2. Verifica su presupuesto antes de realizarlas. 3. Se envía órdenes de compras a varios proveedores con el fin de buscar la opción más conveniente. 4. Selecciona al que más garantías le ofrece. 5. Pide garantías en compras realizadas. 6. Tiene diferentes niveles de autorización de para la mismas. 7. Verifica que cumplan condiciones establecidas al momento de la entrega del socio. 8. Revisa que el documento de transferencia de los bienes o servicios está legalmente autorizado. 9. Registra inmediatamente en su contabilidad las compras realizadas. 10. Controla las compras bajo inventario.	Gerente / Contador / Cajero	Que la institución no envíe órdenes de compras al proveedor. Desconocimiento de mejores garantías. Productos o servicios no cotizados. Productos con características no especificadas.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.2.3 Personas.

Tabla N°26. Cuestionario de identificación de los factores de riesgo para áreas de Personas.

ÁREA OPERATIVA: PERSONAS				
ACTIVIDADES	**PRODUCTOS**	**PROCESO**	**RESPONSABLE**	**FACTOR DE RIESGO**
Establecer políticas, procesos de incorporación, permanencia y desvinculación del personal.	Personal contratado.	1. Debe existir un proceso definido de incorporación del nuevo personal, para que sirva como base y guía para dicha actividad. 2. Antes de cualquier acción se deberá planificar y determinar la/las necesidades de la institución. 3. Realizar el reclutamiento de carpetas necesarias en el tiempo necesario. 4. Seleccionar las carpetas más relacionadas a las necesidades de lainstitución. 5. Realizar las respectivas entrevistas a los seleccionados con el fin de determinar el/la más idóneo/a. 6. Contratar a la persona que cumplió con las características o el perfil de la Institución financiera. 7. Para la incorporación debe tener requisitos de capacitación, entrenamiento, actualización de conocimientos, entrenamiento en diversas especialidades	Gerencia. Presidencia.	No contar con un proceso definido de incorporación del nuevo personal. Que no se realice el reclutamiento respectivo. No seleccionar a la persona más idónea. Que no se contrate al personal adecuado. La institución no planifique las necesidades.
Establecer políticas, procesos de incorporación, permanencia y desvinculación del personal.	Estabilidad del personal.	1. Capacitación y formación de nuevo personal. 2 Evaluación de desempeño 3. Rendición de cuentas 4. Reconocimiento al personal por su desempeño. 5. Seguimiento para determinar el cumplimiento de las funciones asignadas al personal	Gerencia. Consejo de Administración.	No contar con procesos definidos de permanencia del personal, en el cual se evalúe el desempeño, motivación, segregación de funciones y rotación de personal.
	Personal desvinculado.	1. Recibir los elementos suministrados por la compañía, por ejemplo el computador, teléfono, tarjetas de acceso, etc. 2. Realizar una entrevista de salida, la entrevista es muy importante para la compañía ya que provee información para mejorar las condiciones de trabajo , crear programas para retención de empleados, por nombrar algunos beneficios 3. Desafiliar al empleado del sistema de salud, fondo de pensión, retirarlo del pago de nómina 4. Cancelar o deshabilitar los permisos de acceso a información de la compañía que el empleado poseía	Gerencia. Consejo de Administración.	Que no exista procesos formalmente establecidos para la desvinculación del personal. Personal cesado. La desvinculación del personal no se realice por medio del organismo competente.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.2.4 Tecnología de información.

Tabla N°27. Cuestionario de identificación de los factores de riesgo para áreas de Tecnología de información.

ÁREA OPERATIVA: TECNOLOGÍA DE INFORMACIÓN				
ACTIVIDADES	**PRODUCTOS**	**PROCESO**	**RESPONSABLE**	**FACTOR DE RIESGO**
Garantizar que la administración y las operaciones de la TI satisfagan los requerimientos de la	Un plan funcional. Un PO que establezca las actividades de TI. Un responsable de la información. Difusión y comunicación de políticas.	1. Tener apoyo de la Gerencia y Directorio. 2. Contar con un plan funcional de TI alineado con plan estratégico de la institución. 3. Un PO que establezca las actividades a ejecutar de la TI para el logro de objetivo. 4. Un responsable de la información. 5. Difusión y comunicación de políticas, procesos y procedimientos al personal involucrado para asegurar su implementación.	Gerencia de Sistemas	Desconocimiento de plazos de cumplimiento de los planes. Sin un responsable que se encargue de definir, autorizar los accesos y cambios. Custodio de la información sin conocimientos de políticas.
Garantizar que los recursos y servicios provistos	Manuales o reglamentos internos aprobados por el directorio relacionado con la TI.	1. Normas generales del trabajo 2. Normas disciplinarias 3. Forma de organización del trabajo 4. Formas de participación 5. La seguridad social 6. Responsabilidades del uso de las instalaciones de procesamiento de la información.	Gerencia de Sistemas	Desconocimiento de las responsabilidades y procedimientos para la operación. No exista por escrito el uso de las instalaciones de procesamiento de la información. No se encuentre establecido las normas, principios, y lineamientos aplicables en la institución, que establezcan respuestas a incidentes de TI.
Garantizar que el sistema de administración de seguridad satisfaga las necesidades de la institución para salvaguardar la información contra el uso, modificación	Salvaguardar la información contra el uso, modificación no autorizados, daños y pérdidas	1. Crear políticas y procedimientos de seguridad de la información que garanticen las operaciones. 2. Identificación de los requerimientos de seguridad relacionados con la TI 3. Crear controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información. 4. Contar con un sistema de administración de las seguridades de acceso a la información. 5. Tener un Sistemas de control y autenticación para evitar accesos no autorizados. 6. Crear controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia.	Gerencia de Sistemas	Que no cuenten con controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada. No cuente con controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, desinfección de virus informáticos y demás software maliciosos. Que no exista un procedimiento clasificación y control de activos de TI con su respectivo registro identificación así como responsable de su uso y mantenimiento.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.2.5 Eventos externos.

Tabla N°28. Cuestionario de identificación de los factores de riesgo para áreas de Eventos externos.

ÁREA OPERATIVA: EVENTOS EXTERNOS			
ACTIVIDADES	**PRODUCTOS**	**RESPONSABLE**	**FACTOR DE RIESGO**
Contar con planes de contingencia y de continuidad del negocio, en caso de que ocurra algún evento ajeno a su control	Planes de contingencia de continuidad del negocio establecidos.	Gerencia. Concejo de Administración	Fallas en el suministro de energía, Catástrofes naturales, Disturbios civiles, Actos terroristas, Incumplimiento de contratos de terceros, Fraude externo /asalto y robo

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.3 PASO #3: Identificación del origen del riesgo y potenciales consecuencias.

Una vez identificados los factores de riesgo para cada área operativa por actividades, se debe proceder a realizar una descripción de las potenciales consecuencias que se originarían si se concretara el hecho de un factor de riesgo operacional.

4.2.3.1 Generales.

Tabla N°29. Cuestionario de identificación del origen del riesgo para áreas generales.

ÁREA OPERATIVA: GENERALES				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**ORIGEN DEL RIESGO**	**POTENCIAL CONSECUENCIA**
1	Definir la estructura orgánica de acuerdo a los objetivos de la institucion	No se actualice la estructura orgánica. Desconocimiento de los cargos por parte del personal de la entidad.	Endógeno	Ocupar cargos contrarios al perfil. Que las decisiones se tomen por personal no idóneo. Que no conozca su responsabilidad. En las asignaciones exista doble autoridad. Desconocimiento de los diferentes canales de comunicación y supervisión.
2	Definir un proceso de administración de la Información	Errores en el ingreso de la información. Espacio de almacenamiento insuficiente. Que la información difundida sea incorrecta.	Endógeno	Más interés, pagos incorrectos, etc Pérdida de la Información. Pérdida de clientes . Pérdida de la confianza de los socios . Atención al público indeseada.
3	Construir infraestructura que permita alojar recursos físicos relacionados con TI.	Falte espacio físico. Disponibilidad de información y documentación confidencial. Disponibilidad al polvo. No apoyar la continuidad de operaciones. Mayor deterioro del Equipos.	Endógeno	Congestionamiento de recursos físicos. Incomodidad para el personal que labora en esa área. Rotura de equipos. Pérdida de información. Deterioro de documentación física.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.3.2 Proceso.

Tabla N°30. Cuestionario de identificación de los factores de riesgo para áreas de Procesos.

ÁREA OPERATIVA: PROCESOS				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**ORIGEN DEL RIESGO**	**POTENCIAL CONSECUENCIA**
1	Verificación de identidad	Que no se verifique minuciosamente los documentos y firmas de los socios.	Endogeno	Al no revisar minuciosamente los documentos y firmas de los socios/clientes, existe la posibilidad hacer la transacción incorrecta de la operación solicitada por el socio o cliente, Hacer pagos o cobros inadecuados de los mismos.
2	Caja	No se realicen arqueos oportunos de caja. Robos de dinero y documentos mercantiles	Endogeno	No se comprueba si hay faltantes o sobrantes en caja y no se puede comprobar que su manejo haya sido adecuado por parte del custodio del efectivo, dificultando la identificación de hallazgos, para tomar las medidas de control necesarias.
3	Pagos	No contar con su respectiva documentación para el sustento del socio/cliente como para la institución. Que no se emitan comprobantes de las transacciones realizadas.No tener el respaldo de la persona de que hizo la transacción tanto de la Cooperativa como el beneficiario.	Endogeno	área de caja (llaves), está expuesta algún tipo deatraco como robo, ya sea por parte de empleados, clientes o cualquier otra persona.
4	Recaudación	Que el origen de los fondos no sea lícito. Que existan billetes falsos	Endogeno	Entrega de dinero a persona incorrecta; Problemas con las entidades controladoras al no emitir documentos de respaldo de las transacciones efectuadas durante un periodo determinado; Sin respaldo de documentación que sirva para futuras rendición de cuentas.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.3.3 Personas.

Tabla N°31. Cuestionario de identificación de los factores de riesgo para áreas de Personas.

ÁREA OPERATIVA: PERSONAS				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**ORIGEN DEL RIESGO**	**POTENCIAL CONSECUENCIA**
1	Establecer políticas, procesos de incorporación, permanencia y desvinculación del personal.	No contar con un proceso definido de incorporación del nuevo personal.	Endogeno	Contratar a personal no idóneo. No cumpla con las funciones asignadas. No cubrir necesidades de la entidad. Exposición al robo, fraude. Deficiencia en las actividades realizadas por la ineptitud del personal no idóneo dando mala imagen de la institución. Personal no comprometido con el cumplimiento de Objetivos y metas.
		Que no se realice el reclutamiento respectivo.	Endogeno	
		No seleccionar a la persona más idónea.	Endogeno	
		Contratar personal inadecuado.	Endogeno	
		La institución no planifique las necesidades.	Endogeno	
		No contar con procesos definidos de permanencia del personal, en el cual se evalúe el desempeño, motivación, segregación de funciones y rotación de personal	Endogeno	No se demuestra la idoneidad del trabajador. No se demuestra las competencias y resultados del trabajo para lograr los objetivos de la empresa. No permite valorar de la forma más sistemática objetiva posible el rendimiento de los empleados en la organización. Incumplimiento de objetivos. El personal se vuelve indispensable, debido al no existir segregación de funciones.
		Que no exista procesos formalmente establecidos para la desvinculación del personal	Endogeno	Se encuentra más expuesta a los fraudes o errores por la mala segregación del personal, ya que el individuo tenga control sobre dos o más fases de una transacción u operación; No existe la suficiente información, ya que los dos procesos (vinculación con desvinculación), no están relacionados.
		Personal cesado. La desvinculación del personal no se realice por medio del organismo competente.	Endogeno	Demandas contra la institución por parte del personal separado de la misma; pérdida económica; mala reputación de la Cooperativa; despilfarro de tiempo.
2	Garantizar que la administración y las operaciones de la TI satisfagan los requerimientos de la entidad.	Desconocimiento de las responsabilidades y procedimientos para la operación. No exista por escrito el uso de las instalaciones de procesamiento de la información. No se encuentre establecido las normas, principios, y lineamientos aplicables en la cooperativa, que establezcan respuestas a incidentes de TI.	Endogeno	Paralización de las operaciones normales de la empresa por eventos inesperados y que no se puedan solucionar por la ausencia de manuales o reglamentos de las tecnologías de información.
3	Garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades y estén sometidas a un monitoreo.	Desconocimiento de los sistemas a las vulnerabilidades. Sistemas o equipos no estén sometidos a un monitoreo de su Eficiencia y Efectividad. Que la empresa proveedora no cumpla con el contrato o con sus responsabilidades. Que no exista una transferencia del conocimiento. Que no se entregue documentación técnica y de usuario.	Endogeno	Total dependencia con los proveedores externos. Sistemas sin mantener la integridad, disponibilidad y confidencialidad de la información. Retraso en el cumplimiento de las obligaciones con los socios/clientes. Paralización de las actividades de la entidad al presentarse problemas en el sistema.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.3.4 Tecnología de información.

Tabla N°32. Cuestionario de identificación de los factores de riesgo para áreas de Tecnología de información.

ÁREA OPERATIVA: TECNOLOGÍA DE INFORMACIÓN				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**ORIGEN DEL RIESGO**	**POTENCIAL CONSECUENCIA**
1	Garantizar que la administración y las operaciones de la TI satisfagan los requerimientos de la entidad.	Desconocimiento de las responsabilidades y procedimientos para la operación. No exista por escrito el uso de las instalaciones de procesamiento de la información. No se encuentre establecido las normas, principios, y lineamientos aplicables en la cooperativa, que establezcan respuestas a incidentes de TI.	Endogeno	Paralización de las operaciones normales de la empresa por eventos inesperados y que no se puedan solucionar por la ausencia de manuales o reglamentos de las tecnologías de información.
2	Garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades y estén sometidas a un monitoreo.	Desconocimiento de los sistemas a las vulnerabilidades. Sistemas o equipos no estén sometidos a un monitoreo de su Eficiencia y Efectividad. Que la empresa proveedora no cumpla con el contrato o con sus responsabilidades. Que no exista una transferencia del conocimiento. Que no se entregue documentación técnica y de usuario.	Endogeno	Total dependencia con los proveedores externos. Sistemas sin mantener la integridad, disponibilidad y confidencialidad de la información. Retraso en el cumplimiento de las obligaciones con los socios/clientes. Paralización de las actividades de la entidad al presentarse problemas en el sistema.
3	Garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, modificación no autorizada, daños y pérdidas.	No cuente con controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, desinfección de virus informáticos y demás software maliciosos.	Endogeno	Disponibilidad de ataques externos especialmente a la información crítica. Robo de la información contenida ya sea en documentos, medios de almacenamiento, etc. y divulgación no autorizada de la misma afectando la confidencialidad de la misma válida únicamente para los intereses.
		Que no exista un procedimiento de clasificación y control de activos de TI con su respectivo registro e identificación así como responsable de su uso y mantenimiento.	Endogeno	Personal no autorizado dé uso de los activos de TI, al no estar designado. Mayor exposición de error o fraude.
		Que la institución no cuente con instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles.	Endogeno	Ingreso de personal no autorizado. Infiltración en los sistemas. Posible robo, alteración o modificación de la información. Alteraciones de base de datos. Acceso a los sistemas informáticos y de información de forma ilícita. Daño informático. Destrucción a la infraestructura de las instalacion es físicas necesarias para el procesamiento de información.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.3.5 Eventos externos.

Tabla N°33. Cuestionario de identificación de los factores de riesgo para áreas de Eventos Externos.

ÁREA OPERATIVA: EVENTOS EXTERNOS				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**ORIGEN DEL RIESGO**	**POTENCIAL CONSECUENCIA**
1	Contar con planes de contingencia y de continuidad del negocio, en caso de que ocurra algún evento ajeno a su control	fallas en el suministro de energía	Exógeno	Pérdida del trabajo realizado. Paralización de las actividades. Pérdidas económicas. Retraso en las obligaciones.
		Catástrofes naturales	Exógeno	Pérdidas humanas, económicas, bienes destruidos, pérdida de tiempo, etc.
		Disturbios civiles	Exógeno	Paralización de las actividades normales de la enti dad, dando como consecuencia un retraso en las tareas diarias, pérdida de tiempo, dinero.
		Actos terroristas	Exógeno	Trauma en las personas que viven el evento. Víctimas humanas. Pérdidas económicas, pérdidas de documentos e información.
		Incumplimiento de contratos de terceros	Exógeno	Mala reputación de la Cooperativa, pérdida de tiempo por cuestión legal.
		Fraude externo /asalto y robo	Exógeno	Pérdida de información confidencial, que comprometa a la entidad. Pérdidas económicas significativas que paralicen la operatividad de la Cooperativa. Mala imagen de la institución. Consecuencias psicológicas en los emp leados víctimas de estos eventos.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.4 PASO #4: Determinación de la probabilidad de ocurrencia y grado de impacto potencial.

Se debe analizar la probabilidad de que ciertos factores de riesgo de las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero en El Salvador, se materialice el evento no deseado, con diferentes niveles o escalas de probabilidad, y por otra lado el impacto o la consecuencia midiendo el grado de severidad que pueden presentar los daños a la entidad por paralización de los procesos.

4.2.4.1 Generales.

Tabla N°34. Evaluación para determinar la probabilidad de ocurrencia y el grado de impacto potencial en áreas generales.

ÁREA OPERATIVA: GENERALES				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO POTENCIAL**
1	Definir la estructura orgánica de acuerdo los objetivos de la cooperativa.	No se actualice la estructura orgánica.	MEDIA	MEDIO
		Desconocimiento de los cargos por parte del personal de la entidad.	BAJA	MEDIO
2	Definir un proceso de administración de la información.	Errores en el ingreso de la información. Espacio de almacenamiento insuficiente. Que la información difundida sea incorrecta.	ALTA	ALTO
3	Construir infraestructura que permita alojar recursos físicos relacionados con TI.	Falte espacio físico. Disponibilidad de información y documentación confidencial. Disponibilidad al polvo. No apoyar la continuidad de operaciones. Mayor deterioro del Equipos.	MEDIA	ALTO
4	Establecer procedimientos alternativos a la operatividad normal de la entidad.	Pérdida de información. La empresa no pueda reaccionar ante un cambio.	BAJA	ALTO

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.4.2 Proceso.

Tabla N°35. Evaluación para determinar la probabilidad de ocurrencia y el grado de impacto potencial en áreas Procesos.

ÁREA OPERATIVA: PROCESOS				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO POTENCIAL**
1	Caja	No se realicen arqueos oportunos de caja.	BAJA	MEDIO
		Robos de dinero y documentos mercantiles.	ALTA	ALTO
2	Pagos	No contar con su respectiva documentación para el sustento del socio/cliente como para la institución. Que no se emitan comprobantes de las transacciones realizadas. No tener el respaldo de la persona de que hizo la transacción tanto de la Cooperativa como el beneficiario.	BAJA	ALTO
3	Recaudación	Que el origen de los fondos no sea lícito; Que existan billetes falsos.	ALTA	ALTO
4	Cobro de servicios básicos	Cobrar servicio de un usuario diferente.	BAJA	BAJO
5	Verificar que los datos del socio/cliente coincidan con los datos de la remesa y pago de la misma.	Alteración de identidad.	BAJA	MEDIO
		Entrega de dinero a beneficiario diferente.	BAJA	MEDIO

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.4.3 Personas.

Tabla N°36. Evaluación para determinar la probabilidad de ocurrencia y el grado de impacto potencial en áreas Personas.

ÁREA OPERATIVA: PERSONAS				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO POTENCIAL**
1	Establecer políticas, procesos de incorporación, permanencia y desvinculación del personal.	No contar con un proceso definido de incorporación del nuevo personal.	ALTA	MEDIO
		Que no se realice el reclutamiento respectivo.	BAJA	ALTO
		No seleccionar a la persona más idónea.	BAJA	ALTO
		Que no se contrate al personal adecuado.	BAJA	ALTO
		La institución no planifique las necesidades.	MEDIA	MEDIO
		No contar con procesos definidos de permanencia del personal, en el cual se evalúe el desempeño, motivación, segregación de funciones y rotación de personal.	ALTA	MEDIO
		Personal cesado. La desvinculación del personal no se realice por medio del organismo competente.	ALTA	MEDIO

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.4.4 Tecnología de información.

Tabla N°37. Evaluación para determinar la probabilidad de ocurrencia y el grado de impacto potencial en áreas Tecnología de información.

ÁREA OPERATIVA: TECNOLOGÍA DE INFORMACIÓN				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO POTENCIAL**
1	Garantizar que la administración y las operaciones de la TI satisfagan los requerimientos de la entidad.	Desconocimiento de plazos de cumplimiento de los planes. Sin un responsable que se encargue de definir, autorizar los accesos y cambios. Custodio de la información sin conocimientos de políticas.	ALTA	ALTO
		Desconocimiento de las responsabilidades y procedimientos para la escrito operación. No exista por el uso de las instalaciones de procesamiento de la información. No se encuentre establecido las normas, principios, y lineamientos aplicables en la cooperativa, que establezcan respuestas a incidentes de TI.	ALTA	ALTO
2	Garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades y estén sometidas a un monitoreo.	Desconocimiento de los sistemas a las vulnerabilidades. Sistemas o equipos no estén sometidos a un monitoreo de su Eficiencia y Efectividad. Que la empresa proveedora no cumpla con el contrato o con sus responsabilidades. Que no exista una transferencia del conocimiento.Que no se entregue documentación técnica y de usuario.	ALTA	ALTO
3	Garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar contra la información el uso, modificación no autorizada, daños y pérdidas.	Que no cuenten con controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada.	ALTA	ALTO

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.4.5 Eventos externos.

Tabla N°38. Evaluación para determinar la probabilidad de ocurrencia y el grado de impacto potencial en áreas Eventos externos.

ÁREA OPERATIVA: EVENTOS EXTERNOS				
N°	**ACTIVIDADES**	**FACTORES DE RIESGO**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO POTENCIAL**
1	Garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, modificación no autorizada, daños y pérdidas.	No cuente con controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, desinfección de virus informáticos y demás software maliciosos.	ALTA	ALTO
		Que no exista un procedimiento de clasificación y control de activos de TI con su respectivo registro e identificación así como responsable de su uso y mantenimiento.	ALTA	MEDIO
		Que la institución no cuente con instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles.	ALTA	ALTO
		No contar con el servicio de transferencias y transacciones electrónicas.	BAJA	BAJO
		Que no cuente con Información de respaldo y procedimientos de restauración ante eventos de desastre.	ALTA	ALTO

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.5 PASO #5: Valorización, gravedad y respuesta al riesgo.

Una vez determinado la probabilidad e impacto de cada factor de riesgo, se debe determinar la gravedad, la misma que es resultado de la combinación de estas dos variables: Probabilidad e Impacto, seguido de esto daremos la respuesta al riesgo, la que podría ser: Evitar, Reducir o Aceptar. Luego se deben analizar los controles con los que cuentan las instituciones, cuál es su efectividad en valores y calcularemos el promedio de dichos controles de cada factor de riesgo, resultado que servirá para determinar el riesgo residual para proponer medidas correctivas.

4.2.5.1 Generales.

Tabla N°39. Evaluación para valorización, determinación de la gravedad y evaluación al riesgo en áreas generales.

ÁREA DE OPERACIÓN: GENERALES										
N°	**FACTORES DE RIESGOS**	**ANÁLISIS DE RIESGO**			**RESPUESTA AL RIESGO**	**CONTROLES DE LA INSTITUCIÓN**		**RIESGO RESIDUAL = (G) - (E)**	**PRIORIDAD**
		PROBABILIDAD DE OCURRENCIA (P)	GRADO DE IMPACTO POTENCIAL (I)	GRAVEDAD DEL RIESGO (G) = (P)*(I)		CONTROL	EXPOSICIÓN (E)		
1	No se actualice la estructura orgánica	MEDIA	MEDIO	MEDIA	REDUCIR	Reuniones cada año por la asamblea general.	3	1	3
2	Desconocimiento de los cargos por parte del personal de la entidad.	BAJA	MEDIO	MEDIA	REDUCIR	Información de solicitud de crédito.	4	1	3
3	Errores en el ingreso de la información. Espacio de almacenamiento insuficiente. Que la información difundida sea incorrecta.	ALTA	ALTO	ALTA	REDUCIR	Ninguno	1	5	1
4	Falte espacio físico. Disponibilidad de información y documentación confidencial. Disponibilidad al polvo. No apoyar la continuidad de operaciones. Mayor deterioro del Equipos.	MEDIA	ALTO	ALTA	REDUCIR	Ninguno	1	4	1

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.5.2 Proceso.

Tabla N°40. Evaluación para valorización, determinación de la gravedad y evaluación al riesgo en áreas generales.

ÁREA DE OPERACIÓN: PROCESOS										
N°	**FACTORES DE RIESGOS**	**ANÁLISIS DE RIESGO**			**RESPUESTA AL RIESGO**	**CONTROLES DE LA INSTITUCIÓN**			
		PROBABILIDAD DE OCURRENCIA (P)	GRADO DE IMPACTO POTENCIAL (I)	GRAVEDAD DEL RIESGO (G) = (P)*(I)		CONTROL	EXPOSICIÓN (E)	**RIESGO RESIDUAL = (G) - (E)**	**PRIORIDAD**
1	Que no se verifique minuciosamente los documentos y firmas de los socios.	MEDIA	MEDIO	MEDIA	REDUCIR	Pericia del cajero	2	2	3
2	No se realicen arqueos oportunos de caja	MEDIA	MEDIO	MEDIA	REDUCIR	Arqueos de caja diariamente	4	1	3
3	Robos de dinero y documentos mercantiles	ALTA	ALTO	ALTA	REDUCIR	Cada cajero tienela responsabilidad de mantener segura su área de trabajo.	1	5	1
4	No contar con su respectiva documentación para el sustento del socio/cliente como para la institución.Que no se emitan comprobantes de las transacciones realizadas. No tener el respaldo de la persona de que hizo la transacción tanto de la Cooperativa como el beneficiario.	BAJA	ALTO	MODERAI	REDUCIR	El sistema que tiene la Cooperativa no se puede hacer la transacción sin la impresión del comprobante	1	2	2
5	Que el origen de los fondos no sea lícito; Que existan billetes falsos.	ALTA	ALTO	ALTA	REDUCIR	Cuentan con un manual, Contra lavado de Activos	4	1	1

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.5.3 Personas.

Tabla N°41. Evaluación para valorización, determinación de la gravedad y evaluación al riesgo en áreas generales.

ÁREA DE OPERACIÓN: PERSONAS										
N°	**FACTORES DE RIESGOS**	**ANÁLISIS DE RIESGO**				**CONTROLES DE LA INSTITUCIÓN**			
		PROBABILIDAD DE OCURRENCIA (P)	GRADO DE IMPACTO POTENCIAL (I)	GRAVEDAD DEL RIESGO (G) = (P)*(I)	**RESPUESTA AL RIESGO**	CONTROL	EXPOSICIÓN (E)	**RIESGO RESIDUAL = (G) - (E)**	**PRIORIDAD**
1	No contar con un proceso definido de incorporación del nuevo personal.	ALTA	MEDIO	ALTA	REDUCIR	Ninguno	1	5	1
2	Que no se realice el reclutamiento respectivo	BAJA	ALTO	MEDIA	REDUCIR	Reuniones entre Concejo de Administración y Gerencia.	3	3	2
3	No seleccionar a la persona más idónea.	BAJA	ALTO	MEDIA	REDUCIR		3	3	2
4	Que no se contrate al personal adecuado.	BAJA	ALTO	MEDIA	REDUCIR		3	3	2
5	La institución no planifique las necesidades	MEDIA	MEDIO	MEDIA	REDUCIR		3	3	3

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.5.4 Tecnología de información.

Tabla N°42. Evaluación para valorización, determinación de la gravedad y evaluación al riesgo en áreas generales.

ÁREA DE OPERACIÓN: TECNOLOGÍA DE INFORMACIÓN											
N°	**FACTORES DE RIESGOS**	**ANÁLISIS DE RIESGO**				**CONTROLES DE LA INSTITUCIÓN**					
		PROBABILIDAD DE OCURRENCIA	GRADO DE IMPACTO POTENCIAL (I)	GRAVEDAD DEL RIESGO (G) = (P)*(I)	**RESPUESTA AL RIESGO**	CONTROL	EXPOSICIÓN (E)	**RIESGO RESIDUAL = (G) - (E)**	**PRIORIDAD**		
1	Desconocimiento de plazos de cumplimiento de los planes. Sin un responsable que se encargue de definir, autorizar los accesos y cambios. Custodio de la información sin conocimientos de políticas.	ALTA	ALTO	ALTO	REDUCIR	NINGUNO	1	5	1		
2	Desconocimiento de las responsabilidades y procedimientos para la operación. No exista por escrito el uso de las instalaciones de procesamiento de la información. No se encuentre establecido las normas, principios, y lineamientos aplicables en la cooperativa, que establezcan respuestas a incidentes de TI.	ALTA	ALTO	ALTO	REDUCIR	NINGUNO	1	5	1		
3	Desconocimiento de los sistemas a las vulnerabilidades. Sistemas o equipos no estén sometidos a un monitoreo de su Eficiencia y Efectividad. Que la empresa proveedora no cumpla con el contrato o con sus responsabilidades. Que no exista una transferencia del conocimiento. Que no se entregue documentación técnica y de usuario.	ALTA	ALTO	ALTO	REDUCIR	NINGUNO	1	5	1		

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.5.5 Eventos externos.

Tabla N°43. Evaluación para valorización, determinación de la gravedad y evaluación al riesgo en áreas generales.

ÁREA DE OPERACIÓN: EVENTOS EXTERNOS										
N°	**FACTORES DE RIESGOS**	**ANÁLISIS DE RIESGO**			**RESPUESTA AL RIESGO**	**CONTROLES DE LA INSTITUCIÓN**		**RIESGO RESIDUAL = (G) - (E)**	**PRIORIDAD**
		PROBABILIDAD DE OCURRENCIA (P)	GRADO DE IMPACTO POTENCIAL (I)	GRAVEDAD DEL RIESGO (G) = (P)*(I)		CONTROL	EXPOSICIÓN (E)		
1	Fallas en el suministro de energía	MEDIA	ALTO	ALTA	REDUCIR	NINGUNO	1	5	1
2	Catástrofes naturales	BAJA	ALTO	MEDIA	ACEPTAR	NINGUNO	1	4	2
3	Disturbios civiles	BAJA	MEDIO	MEDIA	ACEPTAR	NINGUNO	1	3	3
4	Actos terroristas	BAJA	ALTO	MEDIA	ACEPTAR	NINGUNO	1	4	2
5	Incumplimiento de contratos de terceros	BAJA	ALTO	MEDIA	ACEPTAR	NINGUNO	1	4	2
6	Fraude externo /asalto y robo	MEDIA	ALTO	ALTA	REDUCIR	NINGUNO	1	5	1

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.6 PASO #6: Plan de mitigación de riesgo operacional.

4.2.6.1 Generales.

Tabla N°44. Plan de mitigación de riesgo operacional para áreas generales.

ÁREA: **GENERAL**								
OBJETIVO: **CREAR UN COMITÉ DE GESTÓN INTEGRAL DEL RIESGO.**								
DESCRIPCIÓN DEL RIESGO: **QUE LA INSTITUCIÓN NO CUENTE CON PERSONAL CON COMPETENCIAS SUFICIENTES PARA ELABORAR O EJECUTAR UN PLAN PARA REDUCIR RIESGOS.**								
RESPUESTA AL RIESGO: REDUCIR EL RIESGO								
N°	**MEDIDAS**	**PRIORIDAD**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**			**INDICADORES**
					PLAZO	**INICIO**	**FIN**	
1	Crear un comité de administración de riesgos, o elegir un responsable.	2	GERENCIA. C.ADMINISTRACION.	Gerente. Miembros del concejo de administración.	Prom. 10 días			Verificar el acta de la creación del concejo de administración.
2	Modificar la estructura organizacional como fundamento de las actividades de administración de riesgos.	2	GERENCIA. C.ADMINISTRACION.	Gerente. Miembros del concejo de administración.	Prom. 3 días			Verificar que la estructura organizacional esté actualiza.
3	Establecer políticas por escrito de administración de riesgos acorde a las circunstancias de la institución	2	GERENCIA. C.ADMINISTRACION.	Miembros del comité de riesgo, computadora, impresora, suministros de oficina	Prom. 11 días			Constatar que las políticas estén establecidas, respaldadas por escrito y aprobadas por el concejo de Administración
4	Involucrar a la dirección general en las actividades de administración de riesgos, mediante un acuerdo de la institución.	2	GERENCIA. C.ADMINISTRACION.	Miembros de la asamblea general, del Comité o responsable de administración de riesgos. Reuniones. Firmas de actas y acuerdos.	Prom. 5 días			Constatar que las actas se encuentren firmadas por los involucrados (Dirección General y C.de Administración de Riesgos).

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°45. Plan de mitigación de riesgo operacional para áreas generales.

ÁREA:	**GENERAL**							
OBJETIVO:	CREAR UN CÓDIGO DE ÉTICA.							
DESCRIPCIÓN DEL RIESGO:	QUE LA INSTITUCIÓN NO CUENTE CON UNA NORMATIVA INTERNA DE COMPORTAMIENTO							
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO							
N°	**MEDIDAS**	**PRIORIDAD**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**			**INDICADORES**
					PLAZO	**INICIO**	**FIN**	
1	Establecer una comisión para que realice el código de ética.	1	GERENCIA CONCEJO DE ADMINISTRACIÓN.	Gerente, Miembros del concejo de administración.	Prom.3 días			Verificar el acta de la creación de la comisión de ética.
2	Establecer el documento del código de ética	1	COMISION ENCARGADA DEL CÓDIGO DE ÉTICA.	Miembros de la Comisión de ética, Computador, Suministros de oficina.	Prom.10 días			Verificar que el documento del código de ética este creado y aprobado.
3	Socializar el documento de código de ética, en el cual se establece el comportamiento de lo que es permitido, bueno, malo etc., frente a una decisión o acción.	1	GERENCIA. COMISIÓN ENCARGADA DEL CÓDIGO ÉTICA.	Gerente, Miembros de la C. encargada del Código de Ética, Personal notificado, Suministros de oficina, Computador.	Prom.30 días			Listado de los empleados participantes de las charlas de socialización.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.6.2 Proceso.

Tabla N°46. Plan de mitigación de riesgo operacional para áreas de Procesos.

ÁREA:	**PROCESOS**						
OBJETIVO:	ESTABLECER MEDIDAS DE SEGURIDAD FÍSICA EN LAS ÁREAS DE RECEPCIÓN DEL DINERO.						
DESCRIPCIÓN DEL RIESGO:	SUCESOS DE ROBO DE DINERO Y/O DOCUMENTOS MERCANTILES.						
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO						
N°	**MEDIDAS**	**PRIOR.**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**		**INDICADORES**
					PLAZO	**INICIO** / **FIN**	
1	Instalar protecciones de seguridad en los cajones de recepción de dinero con candados ó cerraduras que contengan códigos para abrirlos.	1	PERSONAL CONTRATODO PARA LA OCASIÓN	Económicos. Persona contratada.	Prom. 30 días	A convenir / A convenir	Total de cajas con protecciones / total de cajas

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°47. Plan de mitigación de riesgo operacional para áreas de Procesos.

ÁREA:	**PROCESOS**						
OBJETIVO:	CREAR UN MANUAL PARA COMPRAS Y PAGOS DE PROVEEDORES						
DESCRIPCIÓN DEL RIESGO:	QUE LA INSTITUCIÓN NO REALICE LAS COMPRAS POR MEDIO DE ÓRDENES DE COMPRAS; QUE NO SE COTICEN LOS PRODUCTOS O SERVICIOS AL MENOS A TRES PROVEEDORES; DESCONOCIMIENTO DE MEJORES GARANTÍAS; ADQUISICIÓN DE PRODUCTOS CON CARACTERÍSTICAS NO ESPECIFICADAS.						
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO						
N°	**MEDIDAS**	**PRIORIDAD**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**		**INDICADORES**
					PLAZO	**INICIO FIN**	
1	El Concejo de Administración delegará una Comisión para la elaboración del manual de compras.	1	CONCEJO DE ADMINISTRACIÓN	Miembros del concejo de administración.	Prom. de 3 días		Verificar la delegación de la comisión
2	La Comisión hará el levantamiento de los procesos de la Institución.	1	COMISIÓN DE LA ELABORACIÓN DEL MANUAL DE COMPRAS	Suministros de oficina. Miembros de la Comisión encargada de lmanual de Computador, Impresora	Prom. de 16 días		Constatar procesos de compras levantados.
3	La Comisión establecerá un documento formal que será aprobado por la Junta General	1	COMISIÓN, ENCARGADO DEL MANUAL DE COMPRAS	Comisión encargada del manual de compras. Computador, de Suministros oficina.	Prom. de 15 días		Verificar el documento de compra aprobado.
4	Socializar a los empleados que se encuentren involucrados en el proceso de compra.	1	GERENCIA. CONSEJO DE ADMINISTRACION	Suministros de oficina, Miembros de la Comisión encargada del manual de compras, Computador, Impresora, Miembros involucrados en el proceso de compra.	Prom. de 6 días		Verificar que los empleados conozcan el proceso de compra.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.6.3 Personas.

Tabla N°48. Plan de mitigación de riesgo operacional para áreas de Personas.

ÁREA:	**PERSONAS**					
OBJETIVO:	ESTABLECER POLÍTICAS, PROCEDIMIENTOS DE INCORPORACIÓN PERMANENTE Y DESVINCULACIÓN DE PERSONAL.					
DESCRIPCIÓN DEL RIESGO:	QUE LA INSTITUCIÓN NO CUENTE CON PROCESO DEFINIDOS PARA LA EVALUACÓN DEL DESEMPEÑO, MOTIVACIÓN DEL PERSONAL Y SEGREGACIÓN DE FUNCIONES.					
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO					
N°	**MEDIDAS**	**PRIORID**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**	**INDICADORES**
					PLAZO / INICIO / FIN	
1	Talento humano o la persona encargada determine y analice las necesidades de la Institución.	3	ENCARGADO DEL RECURSO HUMANO	Miembros de Recursos Humanos	Prom. de 5 días	Cantidad de vacantes requeridos, Verificar necesidades existentes
2	Determinar perfiles que se exigirá a cada cargo.	3	ENCARGADO DEL RECURSO HUMANO	Miembros de Recursos Humanos	Prom. de 12 días	Verificar perfiles acordes al cargo.
3	Realizar el reclutamiento de carpetas.	3	ENCARGADO DEL RECURSO HUMANO	Miembros de Recursos Humanos	Prom. de 30 días	Verificar carpetas recibidas.
4	Seleccionar las carpetas con mayor relación al perfil demandado por la institución.	3	ENCARGADO DEL RECURSO HUMANO	Miembros de Recursos Humanos	Prom. de 1 días	Verificar carpetas recibidas.
5	Realizar las respectivas entrevistas, pruebas, etc., a los/lasseleccionados/as con el fin de determinar, y contratar a la persona que cumple con el perfil que la Institución financiera busca.	3	LA GERENCIA Y ENCARGADO DEL RECURSO HUMANO	Miembros de Recursos Humanos, suministros de oficia y computadoras	Prom. de 5 días	Constatar pruebas realizadas a los aspirantes. Verificar contratos de trabajo.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°49. Plan de mitigación de riesgo operacional para áreas de Personas.

ÁREA:	**PERSONAS**						
OBJETIVO:	ESTABLECER POLÍTICAS PARA EL TRATAMIENTO DE PERSONAL CESADO.						
DESCRIPCIÓN DEL RIESGO:	QUE LA INSTITUCIÓN NO REALICE LA DESVINCULACIÓN DE PERSONAL POR MEDIO DEL ORGANISMO COMPETENTE.						
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO						
N°	**MEDIDAS**	**PRIORID**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**		**INDICADORES**
					PLAZO	**INICIO** / **FIN**	
1	El encargado debe restringir el acceso del empleado antes de especialmente si copiara o notificar el cese y vigilar que el mismo accediera a información privada de la institución, descargara grandes cantidades de datos.	3	ENCARGADA DEL PERSONAL	Cámaras vigilancia. Encargado del personal	Prom. de 180 días	A convenir / A convenir	Verificar cámaras de vigilancia, Constatar con guardia de seguridad.
2	El encargado del personal de la institución observará, conocerá, determinara el motivo de la desvinculación del empleado, y realizará el respectivo trámite por medio de los organismos competentes.	3	ENCARGADA DEL PERSONAL	Persona encargada, Computador. Internet. Personal a desvincularse.	Prom. de 180 días	A convenir / A convenir	Constatar actas de finiquito legalizadas, verificar avisos de salida.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.6.4 Tecnología de información.

Tabla N°50. Plan de mitigación de riesgo operacional para áreas de Tecnología de información.

ÁREA:		**TECNOLOGÍA DE INFORMACIÓN**						
OBJETIVO:		GARANTIZAR QUE LA ADMINISTRACIÓN Y LAS OPERACIONES DE LA TECNOLOGÍA DE						
DESCRIPCIÓN DEL RIESGO:		QUE SE DESCONOZCAN LOS PLAZOS DE CUMPLIMIENTOS DE LOS PLANES; QUE NO SE						
RESPUESTA AL RIESGO:		REDUCIR EL RIESGO						
N°	**MEDIDAS**	**PRIORIDAD**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**			**INDICADORES**
					PLAZO	**INICIO**	**FIN**	
1	Contratar una persona que sea responsable de la Tecnología de Información, que controle las claves de acceso a sistemas y la seguridad, con el objeto de prevenir que personas no autorizadas puedan modificar, leer o borrar información de las bases de datos o realizar transacciones no autorizadas para su procesamiento.	1	GERENCIA, CONCEJO DE ADMINISTRACIÓN.	Gerente, Miembros del concejo de administración. Acta de nombramiento.	Prom. de 5 días	A convenir	A convenir	Verificar contrato
2	Establecer los planes de TI para cumplir la misión y metas de la institución.	1	GERENTE, RESPONSABLE DE TI	Gerente, Responsable de TI. Impresora, Suministros de oficina, Computador.	12 días	A convenir	A convenir	Constatar planes establecidos.
3	Socializar mediante charlas ante toda la institución la política de que no se debe fomentar que se comparta la información de cuentas de usuario o, mejor todavía, debe prohibirse por completo y que todo trabajador debe cerrar el ordenador cuando salga del área de trabajo o utilizará contraseñas para el salvapantallas o para el inicio.	1	RESPONSABLE DE TI. GERENCIA. CONCEJO DE ADMINISTRACIÓN	Responsable de TI. Gerente. Miembros del concejo de Administración.	Prom. de 5 días	A convenir	A convenir	Verificar el acta de las charlas efectuadas. Verificar listado de asistencia a las charlas por partede los empleados.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°51. Plan de mitigación de riesgo operacional para áreas de Tecnología de información.

ÁREA:	**TECNOLOGÍA DE INFORMACIÓN**						
OBJETIVO:	GARANTIZAR QUE LA ADMINISTRACIÓN Y LAS OPERACIONES DE LA T.I. SATISFAGAN LOS REQUERIMIENTOS DE LA INSTITUCIÓN.						
DESCRIPCIÓN DEL RIESGO:	DESCONOCIMIENTO DE LAS RESPONSABILIDADES Y PROCEDIMIENTOS PARA LA OPERACIÓN. NO EXISTA POR ESCRITO EL USO DE LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN. NO SE ENCUENTRE ESTABLECIDO LAS NORMAS, PRINCIPIOS, Y LINEAMIENTOS APLICABLES EN LA COOPERATIVA, QUE ESTABLEZCAN RESPUESTAS A INCIDENTES DE TI.						
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO						
N°	**MEDIDAS**	**PRIOR.**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**		**INDICADORES**
					PLAZO	**INICIO** / **FIN**	
1	El responsable de la Tecnología de la Información elaborará Manuales y reglamentos relacionados con la TI, que contengan normas, principios y lineamientos, que establezcan respuestas a incidentes de TI como responsabilidades y procedimientos para la operación.	1	RESPONSABLE DE LA TECNOLOGÍA DE INFORMACIÓN	Persona encargada de TI. Computador. Suministros de Oficina.	Prom. de 30 días	A convenir / A convenir	Constatar manuales elaborados y aprobados.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.2.6.5 Eventos externos.

Tabla N°52. Plan de mitigación de riesgo operacional para áreas de Eventos externos.

ÁREA:	**EVENTOS EXTERNOS**						
OBJETIVO:	CONTAR CON PLANES DE CONTINGENCIA Y DE CONTINUIDAD DEL NEGOCIO, EN CASO DE QUE OCURRA ALGÚN EVENTO AJENO A SU CONTROL.						
DESCRIPCIÓN DEL RIESGO:	FALLAS EN EL SUMINISTRO DE ENERGÍA						
RESPUESTA AL RIESGO:	REDUCIR EL RIESGO						
N°	**MEDIDAS**	**PRIOR.**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**		**INDICADORES**
					PLAZO	**INICIO** / **FIN**	
1	El encargado de compras analizará los requerimientos de la institución, y verificará las necesidades como las características del generador de energía.	1	PERSONA ENCARGADA DE COMPRAS	Encargado de compras	PROM. 60 DÍAS		Verificar el generador eléctrico.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

Tabla N°53. Plan de mitigación de riesgo operacional para áreas de Eventos externos.

ÁREA:	**EVENTOS EXTERNOS**						
OBJETIVO:	**CONTAR CON PLANES DE CONTINGENCIA Y DE CONTINUIDAD DEL NEGOCIO, EN CASO DE QUE OCURRA ALGÚN EVENTO AJENO A SU CONTROL.**						
DESCRIPCIÓN DEL RIESGO:	**FRAUDE EXTERNO /ASALTO Y ROBO**						
RESPUESTA AL RIESGO:	**REDUCIR EL RIESGO**						
N°	**MEDIDAS**	**PRIOR.**	**RESPONSABLE**	**RECURSOS**	**TIEMPO**		**INDICADORES**
					PLAZO	**INICIO** / **FIN**	
1	El encargado de compras analizará los requerimientos de la institución, y verificará las necesidades como las cámaras de seguridad.	1	GERENCIA, CONCEJO DE ADMINISTRACIÓN	Gerencia, Concejo de administración.	PROM.20 DÍAS	A convenir / A convenir	Verificar la existencia física de cámaras de seguridad.
2	Contar con guardias de seguridad en todas las oficinas de la institución.	1	VIGILANCIA, GERENCIA, CONCEJO DE ADMINISTRACIÓN	Vigilancia, gerencia, Concejo de administración.	PROM.30 DÍAS	A convenir / A convenir	Constatar contratos.

Elaborado por: Las autoras. Fuente: (Salinas Zhunio, 2012).

4.3. Propuesta para elaboración de un plan de continuidad del negocio en instituciones financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona occidental.

4.3.1 Propuesta para la elaboración de un plan de continuidad del negocio.

Un Plan de Continuidad de Negocio se compone de varias fases que inician con un análisis de los procesos que componen a la institución. Este análisis servirá para priorizar qué procesos son críticos para la institución y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan a la institución, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Para el Banco Central de Reserva de El Salvador la Gestión de la Continuidad del Negocio es el Proceso de gestión integral que identifica amenazas potenciales a una entidad y el impacto que podrían causar tales amenazas a las operaciones del negocio, en caso de materializarse. Este proceso provee un marco para construir la capacidad organizacional de sobreponerse a un evento disruptivo y ofrecer una respuesta efectiva, de tal manera de salvaguardar los objetivos corporativos, reputación, marca y actividades de creación de valor.

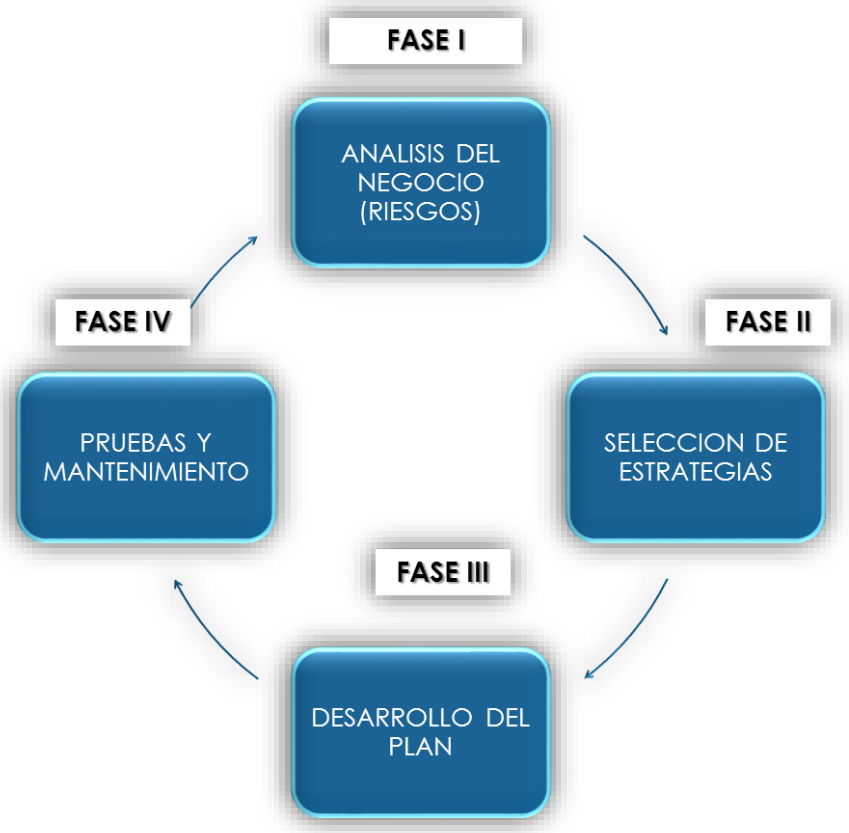
4.3.2 Fases del plan de continuidad del negocio.

Un Plan de Continuidad de Negocio, a diferencia de una Plan de Contingencia está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

Para desarrollar un Plan de Continuidad de Negocio se debe iniciar por obtener un conocimiento de la Institución, sus servicios, sus objetivos empresariales, procesos internos, etc.

El propósito general de un Plan de continuidad es obtener un mapa de acciones que reduzcan "la toma de decisiones" durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costos y aumentando la efectividad.

Ilustración N° 17: Fases del plan de continuidad del negocio



Elaborado por: Las autoras. Fuente: Guía de desarrollo de plan de continuidad del negocio, Laura del Pino.

4.3.1.1 FASE I: Análisis del negocio- BIA (Business Impact Analysis) y evaluación de riesgos.

Esta fase permite conocer y entender cuáles son los procesos de negocio que son esenciales dentro de la institución, con el objetivo de asegurar, la continuidad de la actividad en caso de contingencia. Además permite analizar los impactos que puede causar el no ejecutar un procedimiento por encontrarse ante un incidente o desastre. También ayuda a estimar el tiempo durante el cual un procedimiento puede estar sin operar antes de sufrir impactos considerables para la Institución. Con base en ello, se fija un Tiempo de Recuperación Objetivo (RTO). Para ello se deben de realizar ciertas preguntas, las cuales se pueden responder durante el en el proceso de construcción de la matriz de riesgo operacional, a continuación ejemplo de las preguntas necesarias:

- ¿Cuáles son las actividades más importantes para la institución?
- ¿Cómo afectaría económicamente una interrupción de los servicios a medida que va pasando el tiempo sin reanudar el servicio?
- ¿Cuál sería la capacidad operativa de la institución a medida que pasa el tiempo?
- ¿Cuál es el plazo máximo para volver a la normalidad sin llegar a incurrir en graves pérdidas?

Las actividades o procesos que se clasifican como esenciales en las instituciones suelen ser en su mayoría los Operacionales. Estos procesos interactúan directamente con los clientes o con otras instituciones externas a la institución. Para conocer cuáles son las necesidades de la institución en cuanto a estrategias de continuidad, se utilizaran dos mecanismos de análisis:

4.3.1.1.2 Análisis de impacto (BIA – Business Impact Analysis):

Permitirá identificar la urgencia de recuperación de cada función de institución, determinando el impacto en caso de interrupción. Esta información permitirá seleccionar cuál es la estrategia más adecuada. Ver Anexo 1.

4.3.1.1.3 Análisis de riesgos

El Objetivo de un análisis de riesgos es identificar y analizar los diferentes factores de riesgo que potencialmente podrán afectar a las actividades que se quieren proteger. La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el impacto que supondría para la institución. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado. Ver Anexo 2. Los impactos contemplados son:

- **Regulatorio**/Legal: Incluye pérdidas por no presentar reportes financieros o de impuestos en las fechas indicadas, demandas o penalizaciones al incumplir requerimientos obligatorios en las actividades de la Institución.
- **Financiero**: Incluye pérdida de ingresos, pérdida de intereses, costos de pedir dinero prestado para hacer caja, pérdida de ingresos por préstamos no realizados, penalizaciones por no cumplir compromisos contractuales o niveles de servicio y pérdidas de oportunidades durante el tiempo inoperante.
- **Reputacional**: Incluye la pérdida de confianza por parte de los clientes, del mercado y de los entes de Control, reclamaciones de responsabilidad, clientes insatisfechos por el servicio, apariciones en las noticias por quejas de los clientes y pérdida de reputación.

- **Servicio al cliente**: Incluye el deterioro del servicio al cliente que impide la adecuada y oportuna atención a las necesidades de los usuarios.
- **Operativo**: Incluye la suspensión de la operación y los reproceso que ello puede ocasionar.

Adicional, existe la pregunta referente a sí el procedimiento analizado proporciona información crítica para cualquier otro procedimiento, con el fin de determinar interdependencias. Como resultado de la evaluación se genera las siguientes valoraciones:

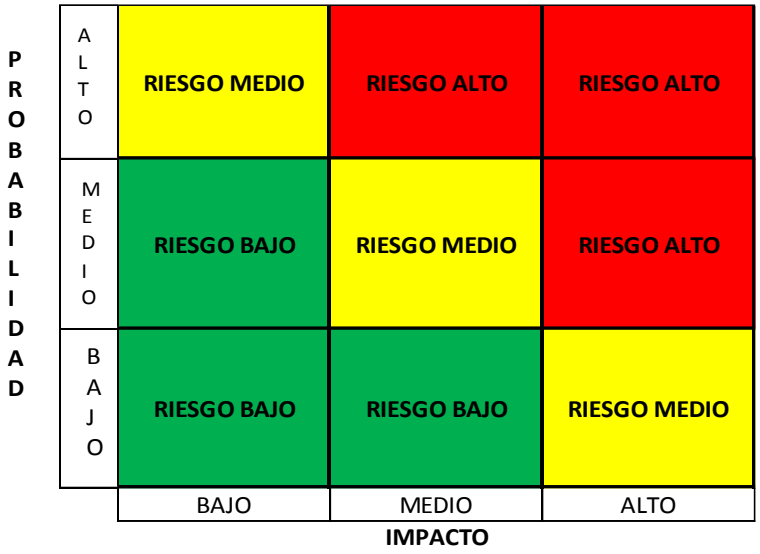
Calificación BIA: Indica la sensibilidad en tiempo ante los diferentes impactos analizados por no ejecutarse el procedimiento. Se realiza en base a los resultados del cuestionario BIA. Ver anexo 2.

Tiempo Objetivo de Recuperación (RTO): El período de tiempo después de una interrupción, mediante el cual la Institución debe activar sus planes de continuidad y recuperación de las actividades críticas para evitar un impacto significativo.

Valor del BIA: Indica la criticidad del procedimiento basado en la Calificación BIA y que impulsa el establecimiento de prioridades de recuperación durante una situación difícil.

Como resultado de esta fase es muy importante construir la matriz del análisis de impacto la cual suele expresar el riesgo en términos cualitativos (alto, medio y bajo), la cual es similar a la desarrollada en la matriz de riesgo operacional:

Ilustración N°18: Resultados de la probabilidad de según la matriz de riesgo operacional



Elaborado por: Las autoras. Fuente: Guía de desarrollo de plan de continuidad del negocio, Laura del Pino.

Ilustración N°19: Clasificación de la probabilidad de ocurrencia del factor de riesgo

CLASIFICACIÓN DE LA PROBALIDAD DE OCURRENCIA DEL FACTOR DE RIESGO				
CONTINGENCIA	**PARÁMETRO DE PROBABILIDAD**	**FRECUENCIA DEL SUCESO DE RIESGO**	**PUNTUACIÓN**	**CLASIFICACIÓN**
Terremoto en ciudades situadas fuera de fallas sísmicas	Podría ocurrir sólo en circunstancias excepcionales.	Una vez cada 10 años o menos frecuente.	**1**	**BAJA**
Robo de información confidencial institucion con control de acceso	Podría ocurrir alguna vez.	Una vez cada 3 o 5 años.	**2**	**MEDIA**
Robo de información confidencial institucion sin control de acceso lógico	Ocurriará alguna vez.	Una vez cada año o mensualmente.	**3**	**ALTA**

Elaborado por: Las autoras. Fuente: Guía de desarrollo de plan de continuidad del negocio, Laura del Pino.

4.3.1.2 FASE II – Selección de estrategias.

En esta fase se seleccionarán los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en la institución. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto. Existen diferentes estrategias para mitigar el impacto de una interrupción. Cada una de estas estrategias tiene unos parámetros de tiempo, disponibilidad y costos asociados que serán más o menos apropiados dependiendo de las funciones de la institución. A continuación se describen diferentes estrategias de reubicación:

- **No hacer nada**: Este tipo de actuación podría utilizarse en aquellas funciones o actividades que se han clasificado como "no urgentes" en el Análisis de Impacto. En este tipo de estrategia se asume el riesgo.
- **Utilización de espacios propios**: Espacios existentes en la institución tales como salas de formación, cafeterías, etc. Este tipo de estrategia requiere una planificación minuciosa.
- **Reutilización de recursos**: Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad. En este caso se debe poner cuidado en convertir la función no urgente en urgente por ser desatendida durante demasiado tiempo.
- **Trabajo remoto o teletrabajo**: Posibilidad de trabajar desde ubicaciones exteriores a la institución mediante conexión remota.
- **Acuerdos recíprocos**: Acuerdos entre dos instituciones (o dos unidades de negocio de la propia institución) con características de equipamiento o espacio similares que permitiría a cada una de las partes recuperar funciones en la otra localización. En este caso es importante definir las condiciones de uso y la realización de pruebas periódicas para asegurar las condiciones pactadas.

- **Sitio alternativo subcontratado a terceros**: Contratación con instituciones especializadas de espacios alternativos para la recuperación de la actividad. En este caso hay que asegurar que estas instituciones pueden proporcionar unos tiempos de recuperación acordes con las necesidades de la institución. Este tipo de instituciones pueden proporcionar diferentes de soluciones:
    a) **Espacio dedicado**: Se garantiza la disponibilidad inmediata del espacio. En contrapartida este servicio es más caro que otras alternativas.
    b) **Espacio compartido**: Se comparte el espacio con otras instituciones. Es más barato que un centro dedicado.
    c) **Espacios móviles**: Se pueden utilizar rápidamente, pero tienen un espacio limitado.
    d) **Módulos prefabricados**: Pueden tardar unos días en estar disponibles para su uso.
- **Centro replicado**: Solución que permite trasladar de forma inmediata la operación y continuar la actividad de forma inmediata.

También puede denominarse "centro espejo". Esta solución es normalmente la más cara, pero también la mejor solución en el caso de que se necesite una recuperación muy rápida de la operación.

A continuación se muestra una tabla que recoge la relación entre el Tiempo Objetivo de recuperación y la solución de continuidad más adecuada a este Objetivo:

Ilustración N°20: Estrategias de recuperación

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
MESES	Reconstrucción /Alojamiento	---
SEMANAS	Edificios prefabricados On-site	Contratación de unidades móviles o prefabricados
DIAS	Recuperación "in situ" trabajo en casa	Subcontratación de procesos en oficinas móviles
HORAS	Localizaciones diversas con empleados formados	Re-localización de un grupo de personas
INMEDIATO	Localizaciones diversas para la misma función	Cambio de funcionamiento a un centro de respaldo subcontratado

Elaborado por: Las autoras. Fuente: Business Continuity Institute.

De todas las alternativas existentes hay que elegir la más adecuada en cada caso, dependerá de las necesidades de la institución, en cuanto a tiempos de recuperación, costos económicos, recursos, etc. Además deberá considerarse otros factores como:

- Ubicación y superficie requerida: Espacio suficiente y zonas acondicionadas para acoger a personal.
- Recursos técnicos necesarios: Hardware, Software, Comunicaciones, Datos de respaldo.
- Recursos humanos requeridos: Recursos materiales y de infraestructura, Servicios auxiliares necesarios, Tiempos de activación y Costos.

Suele ocurrir que cuanto menor sea el tiempo de recuperación objetivo, mayor será el costo de la solución. Por ello es conveniente realizar un análisis con tiempos de recuperación adecuados y adaptados a la realidad de la institución.

Una vez tomada la decisión sobre el tipo de estrategia que se utilizará como respaldo en caso de interrupción de la institución, se pasara a desarrollar todos los procedimientos, funciones y actividades que permitirán restablecer los procesos de la institución en unos plazos razonables.

4.3.1.3 FASE III- Desarrollo del plan de continuidad del negocio.

Hasta este momento se ha obtenido, conocimiento de los procesos de la institución valorando cuáles son críticos para su funcionamiento, se han valorado los riesgos que pueden afectar a la institución y que pueden disparar el Plan de Continuidad de Negocio y se ha definido la estrategia de Continuidad más adecuada para la institución. A partir de aquí se desarrollara "El Plan de Continuidad del Negocio". Para ello se definirá: Los equipos necesarios para el desarrollo del Plan, Las responsabilidades y funciones de cada uno de los equipos, Las dependencias orgánicas entre los diferentes equipos, El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan de Continuidad del Negocio, Los procedimientos de actuación ante incidentes, La estrategia de vuelta a la normalidad.

4.3.1.3.1 Organización de los equipos.

Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan de continuidad del negocio. Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se muestran algunos ejemplos de los equipos que pueden formar parte del Plan:

- Comité de Crisis (Comité de Riesgos): Encargado de dirigir las acciones durante la contingencia y recuperación. Para el caso si la estructura organizativa o el tamaño de la

institución no permita la creación de este Comité, las funciones correspondientes podrán ser desarrolladas por una unidad administrativa que la Junta Directiva designe, procurando cumplir con lo dispuesto.

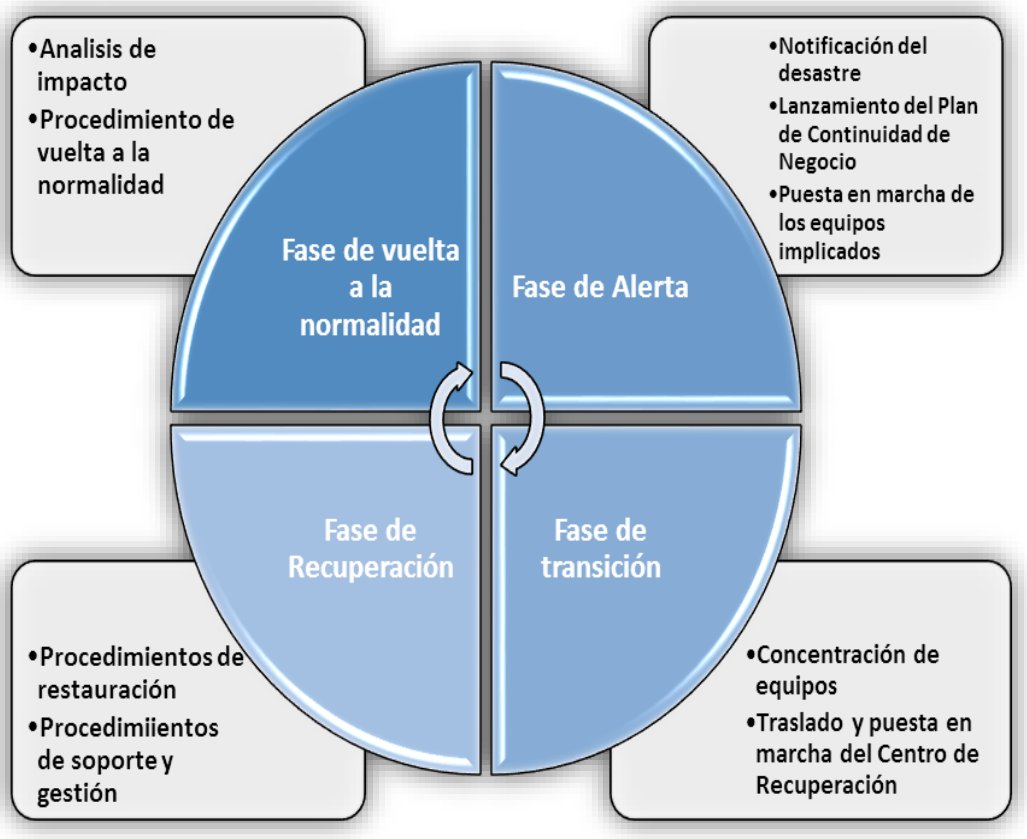
- Equipo de Recuperación (Unidad de Riesgo): Su función es restablecer todos los servidores, computadoras, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio.
- En el caso que la estructura organizativa o el tamaño de la institución no permitan la creación de esta unidad, las funciones correspondientes podrán ser desarrolladas por una unidad administrativa que la Junta Directiva designe.
- Equipo Logístico: Responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como: Transporte de material y personas (si es necesario) al lugar de recuperación, Suministros de oficina, Comida, Reservas de hotel, si son necesarias y Contacto con los proveedores. Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas.
- solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son: Elaboración de comunicados para la prensa y Comunicación con los clientes. Uno de los valores más importantes de una Institución Financiera son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.

4.3.1.3.2 Desarrollo de procedimientos.

Una vez se han definido los equipos y se han establecido las funciones que debe desempeñar cada equipo, se tienen que desarrollar los procedimientos que van a seguir y su actuación en cada una de las fases de activación del Plan de Continuidad. En el siguiente esquema se pueden ver las fases del desarrollo del Plan de Continuidad de Negocio.

4.3.1.3.3 Fases y actividades del desarrollo del plan de continuidad.

Ilustración N°21: Fase y actividades del desarrollo del plan de continuidad



Elaborado por: Las autoras. Fuente: Guía de desarrollo de plan de continuidad del negocio, Laura del Pino.

4.3.1.3.3.1 Fase de alerta.

La Fase de Alerta define los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos. Se dividirá esta fase en tres partes:

- **Notificación**: Define cómo y quién debe ser informado en primera instancia de lo ocurrido.

- **Evaluación**: Análisis de la situación y valoración inicial de los daños.
- **Ejecución del Plan**: Decisión del equipo director de disparar el Plan debido al alcance de los daños.

Notificación: Dado que no es posible elaborar un Plan de Alerta que se adapte a todos los casos que resultan, es de suponer que cualquier persona pueda dar aviso de un incidente, se va suponer que la persona que descubre la contingencia será un empleado o cualquier otra persona próxima al lugar donde ocurre el incidente. Como parte del Plan de continuidad se debe establecer un programa de concienciación, en el que se informe debidamente al personal de cómo actuar ante estos casos y a quién comunicar lo ocurrido.

Ilustración N°22: Fase de notificación

#	EVENTO	ACCIÓN
1	Situación de contingencia/incidente detectado por algún empleado de la compañía. (Fuego, inundación, virus, etc.).	Aviso inmediato con el **máximo detalle posible** al Responsable de Personal de turno o a Seguridad.
2	El responsable de turno o de seguridad conoce que ha sucedido una contingencia.	Aviso a la persona de contacto del Comité de Crisis
		Aviso a los equipos de emergencia (si procede)

Elaborado por: Las autoras. Fuentes: Business Continuity Institute.

Evaluación: Una vez que un miembro del Comité de Crisis es contactado e informado del incidente, procederá a evaluar la situación con la recopilación de la mayor información posible. El Comité informará a los responsables de los distintos equipos de lo ocurrido y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de disparar el Plan Continuidad de Negocio o iniciar otro tipo de estrategia.

Ilustración N°23: Fase de evaluación

#	EVENTO	ACCIÓN
3	Conocimiento por algún miembro del Comité de incidente ocurrido.	El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad del Negocio. Será necesario informar de la situación a los siguientes responsables: • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación. • Responsable de los Equipos.

Elaborado por: Las autoras. Fuentes: Business Continuity Institute.

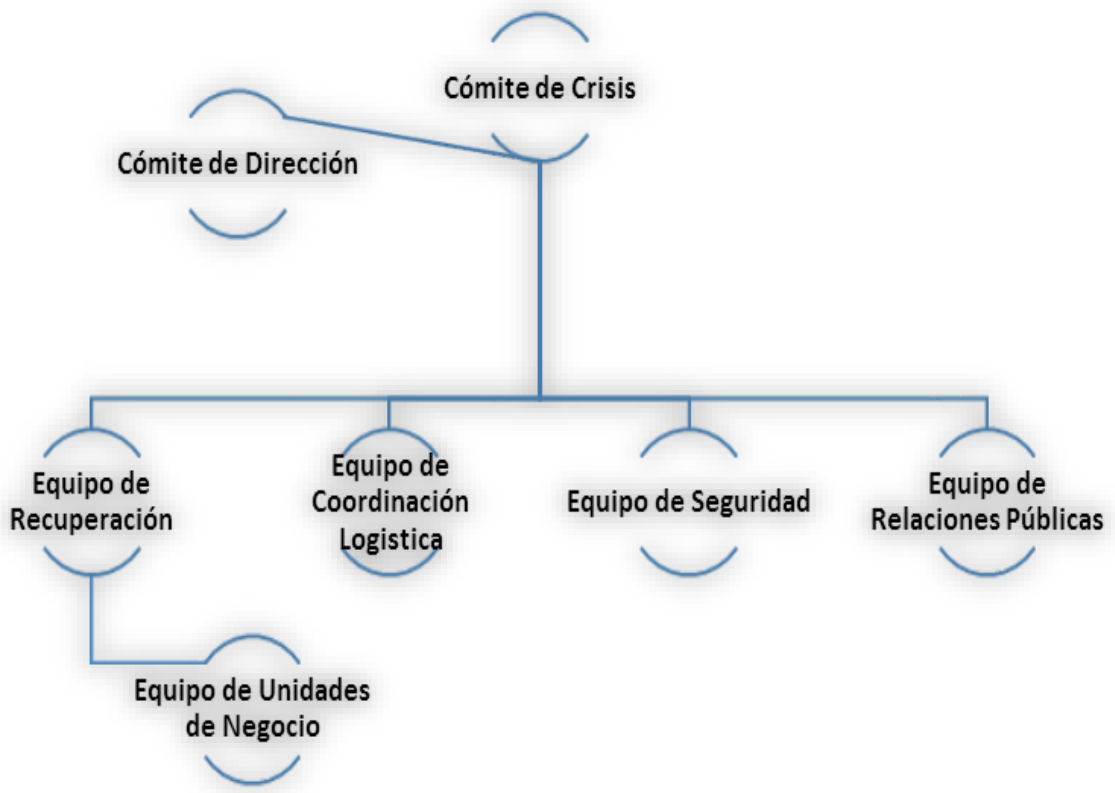
Ejecución del Plan: Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Recuperación, debe de iniciarse el árbol de llamadas, para comunicar a los Responsables y componentes de cada equipo la situación de inicio de las actividades del Plan de Continuidad del Negocio para comenzar los procedimientos de actuación de cada uno de ellos. Deberá informarse también a la Dirección.

Ilustración N° 24: Fase de lanzamiento del plan

#	EVENTO	ACCIÓN
4	Consideración por parte del Comité de Crisis y ejecución del Plan.	Iniciar el árbol de llamadas. Informar al Comité de Dirección
5	Paso a la Fase de Transición	

Elaborado por: Las autoras. Fuentes: Business Continuity Institute.

Ilustración N°25: Árbol de llamada



Elaborado por: Las autoras. Fuente: Guía de desarrollo de plan de continuidad del negocio, Laura del Pino.

4.3.1.3.3.2 Fase de transición.

La Fase de Transición es la fase previa a la de recuperación de los sistemas. Es importante que en esta fase exista una coordinación entre los diferentes equipos incluyendo el equipo de logística, ya que son éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible. Se puede dividir la fase de transición en dos partes:

a) Procedimientos de concentración y traslado de personas y equipos.

b) Procedimientos de puesta en marcha del centro de recuperación.

Ambos procedimientos son la base del proceso de recuperación de los sistemas. Si esta parte falla, no será posible comenzar la recuperación, y por tanto el Plan de Continuidad fallará. Ver Anexo 2. A continuación se describen de manera detallada cada uno de los procedimientos y equipos que deben interactuar en esta fase de transición.

a) Procedimientos de concentración y traslado de material y personas

Dependiendo de la solución final que se decida como estrategia de respaldo, este procedimiento puede variar. Se realizara una descripción general de los procedimientos, que podrá completarse una vez que se tome una solución definitiva. Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al centro de reunión. En el caso de que la emergencia se declare en horas de trabajo, se tomará como punto de encuentro los lugares designados en el Plan de Emergencia. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el Comité de Crisis. (cintas de back up, material de oficina, documentación, etc.)

b) Procedimientos de puesta en marcha del centro de recuperación.

Una vez concentrados los distintos equipos que van a intervenir en la recuperación y con todos los elementos necesarios disponibles para comenzar la recuperación, hay que poner en marcha este centro, estableciendo la infraestructura necesaria, tanto de software como de comunicaciones, etc.

4.3.1.3.3.4 Fase de recuperación.

Una vez se han establecido las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los

mayores esfuerzos e intervenciones para cumplir con los plazos fijados. Se puede dividir esta fase en dos:

- **Procedimientos de Restauración**: Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.
- **Procedimientos de Gestión y Soporte**: Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

4.3.1.3.3.4 Fase de vuelta a la normalidad-fin de la emergencia.

Una vez con los procesos críticos en marcha y solventada la contingencia, se deben plantear las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello se divide esta fase en diferentes procedimientos:

a) Análisis del impacto.
b) Procedimientos de vuelta a la normalidad

a) Análisis del impacto: El análisis de impacto pretende realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.

b) **Procedimientos de vuelta a la normalidad:** Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento. Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

Generación de informes y evaluación

Una vez solventado el incidente y vuelto a la normalidad, cada equipo deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, etc. Toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos y en su caso, tenerlos en cuenta para la adecuación del mismo. Ver Anexo 3.

4.3.1.3 FASE IV: pruebas y mantenimiento.

4.3.1.3.1 Pruebas.

Una parte importante del Plan de Continuidad, es conocer que realmente funciona y es efectivo. Para ello se define la estrategia de pruebas y se realiza la prueba del Plan, para afinarlo según los resultados. Además, en esta última fase se definirán los procedimientos de mantenimiento del Plan.

El Plan de Pruebas diseñado tiene como objetivos:

- Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la institución.
- Probar la efectividad y los tiempos de respuesta del Plan para comprobar que están alineados con la definición realizada en el diseño.
- Identificar las áreas de mejora en el diseño y ejecución del Plan.
- Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.

- Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.
- Concienciación y formación para los empleados a través de la realización de pruebas.

4.3.1.3.2 Tipos de pruebas.

Las pruebas de un Plan de Continuidad deben tener dos características principales:

Realismo: La utilidad de las pruebas se reduce con la selección de escenarios irreales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.

Exposición Mínima: Las pruebas deben diseñarse de forma que impacten lo menos posible en la institución, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible para la institución. En algunos casos puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocio. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo.

4.3.1.3.3. Ejercicios técnicos.

Este tipo de ejercicio requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos verificados durante un ejercicio de simulación son: procedimientos de emergencia, métodos alternativos, líneas de telecomunicaciones de back up, procedimientos de notificación clientes, capacidad y rendimiento del hardware, portabilidad

del software, accesibilidad al centro de respaldo, movilización de los equipos de trabajo, recuperación de ficheros y documentación almacenados en lugar externo, recuperación de datos.

4.3.1.3.4 Mantenimiento del plan de continuidad.

Por la propia dinámica de la institución, se van incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas. La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

4.3.1.3.4 Ejemplos de procedimientos para manejo de incidentes o plan de continuidad del negocio.

Procedimiento de manejo de incidentes por problema en los sistemas.

Objetivos

- Definir un procedimiento para resolver un incidente o problema presentado en los sistemas o aplicativos que manejan la información en sistema de la institución.
- Definir responsabilidades en cuanto a la declaración de contingencias por incidentes o problemas presentados.

Impacto: Alto

Escenario: La contingencia se presenta cuando el hardware y/o software presenta fallas, o cuando haya interrupción prolongada de telecomunicaciones.

Afectación: El sistema almacena información de alta importancia tanto de los clientes como de la Institución, lo que hace necesario resguardarla de manera confidencial, contar con controles y un respaldo por cualquier eventualidad que ocurra en la red.

Acción: Brindar mantenimiento oportuno y crear una copia de contingencia para información de la institución. A continuación se detalla el procedimiento para el manejo de incidentes por problemas en los sistemas:

Comité de crisis

1. Detalla en forma precisa el evento o incidente que se presenta e informa al Líder de Plan de continuidad del Negocio de la dependencia.
2. Verifica si el mismo evento se le está presentando a otros colaboradores de la misma área y si sus tareas afectan a otras dependencias, se debe validar con las mismas si el problema es general.
3. Una vez tenga claridad sobre el evento que se está presentando y los colaboradores involucrados, debe clasificarlo teniendo en cuenta las siguientes definiciones para determinar si es un incidente o un problema:

Incidente: Afecta puntualmente a una persona o grupo de personas.

Problema: Afecta de manera general a todos los usuarios de la institución.

Equipo de recuperación

4. Ingresa en el aplicativo de reporte de incidencias de la Institución. Esto con el fin que la Dirección pueda dejar reportado el evento en el Control de Incidentes.

5. Realiza llamada al Jefe de Riesgos y Coordinador de Infraestructura de la Dirección de Tecnología e informa el incidente de Plan de continuidad del Negocio.
6. Define la solución al incidente (tiempo y estrategia de recuperación) y da respuesta sobre la gravedad del evento y tiempo de recuperación. Si el daño es importante, el Director de Tecnología decide la activación del plan de continuidad de tecnología afectado (servidores backup, sistemas de recuperación de información, enlaces de comunicación), e informa al Director de Continuidad Alterno (Jefe de Riesgos). Director de Continuidad Alterno (Jefe de Riesgos)
7. Informa la situación al Líder de Plan de continuidad del Negocio del área afectada.

Comité de crisis

8. Desarrolla la estrategia

Equipo de recuperación (unidad de riesgo)

9. Una vez solucionado el incidente o problema por parte de la Dirección de Tecnología, informa al Director de Continuidad Alterno (Jefe de Riesgos) y al líder plan de continuidad del negocio del área afectada para que se levante la contingencia.

Comité de crisis

10. Solicita levantar la contingencia del incidente presentado y retorno a la normalidad.
11. Asegura el retorno a la normalidad de las operaciones de acuerdo con el numeral de "Retorno a la normalidad" de la estrategia manual establecida, ejecuta las acciones que permitan que los clientes no se vean afectados en los procesos del área, así como los reportes a entes reguladores.

Procedimiento de escenario de contingencia a sitio alterno.

Objetivos:

- Definir un procedimiento para resolver un incidente o problema presentado en el edificio utilizado por la institución.
- Definir responsabilidades en cuanto a la declaración de contingencias por incidentes o problemas presentados.

Impacto: Alto

Escenario: La contingencia se presenta y se hace necesario el traslado temporal de las operaciones de la institución

Afectación: Operaciones bajo la edificación normal de la institución

Acción: Se debe manejar un adecuado método de traslado de las operaciones claves de la institución, así como el método adecuado de información

A continuación se detalla el procedimiento para el manejo de incidentes por uso de sitio alterno:

Comité de Crisis

1. Activa la contingencia a sitio alterno.
2. Activa la cascada telefónica y comunica el evento de incidente de acuerdo al árbol de llamadas previamente establecido.

Equipo Logístico

3. Contacta a los proveedores de las alternativas seleccionadas, definen el sitio alterno en el cual se mantendrá la operación de la Institución en momento de contingencia.
4. Acuerda con el proveedor la utilización de sus instalaciones por el período de tiempo que dure la contingencia, según las necesidades en ese momento.
5. Coordina el traslado del personal al centro de operaciones establecido para operar en contingencia.

Equipo de las Unidades de Negocio

6. Convoca al personal identificado como personal crítico (equipo de recuperación), e informa el incidente ocurrido, solicitando el desplazamiento al "Lugar alterno de trabajo". El equipo de recuperación se encuentra detallado en el documento "Cascada Telefónica", que posee el Líder de PCN de cada área.
7. Una vez instalados en el centro de operaciones alterno, realiza un chequeo del personal mínimo que se encuentra en el sitio, en caso de ser necesario llamará al personal suplente requerido.

Equipo de Recuperación (Unidad de Riesgo)

8. Solicita el kit de contingencia (recursos de escritorio) y al personal crítico que inicie la conectividad a los programas requeridos.
9. Confirma al Director del comité de crisis la correcta continuidad de los procesos.
10. Realiza una evaluación del sitio alterno, para validar que los recursos requeridos se encuentren disponibles en el sitio.

Equipo de Crisis

11. Solicita a los diferentes Coordinadores de Recuperación un estado del evento y como ha transcurrido la operación en contingencia, se debe de usar el formato de formato de incidentes Anexo 3.

12. El Comité analiza los resultados del estado de la contingencia y procede a decidir:

- "NO" terminar la contingencia: Los equipos de recuperación deben seguir ejecutando la operación en contingencia.
- "SI" terminar la contingencia: Basado en la información suministrada por los Coordinadores y el análisis realizado por los miembros del Comité, el Director de Equipo de Crisis decide terminar la contingencia, da la orden de activar el proceso de retorno.

Coordinadores de Equipos

13. Devuelve el "kit de contingencia" para su custodia nuevamente.

14. Comunicar al personal que participó en la contingencia, el "Retorno a la normalidad" y coordina el desplazamiento al "Sitio base de trabajo".

Capítulo V: Conclusiones y recomendaciones

5.1 Conclusiones

1. Las instituciones Financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, han tenido un nivel de expansión bastante rápido en los últimos años, debido a la necesidad de recursos a nivel personal como de la micro y pequeña empresas, lo que las convierte después de los bancos y cajas de crédito en el principal subsector de intermediación financiera del país.

2. El uso de la tecnología y sistemas de información en las Instituciones financieras no supervisadas es un aspecto fundamental dentro de sus operaciones así como el manejo y capacitación del personal, control interno y mejoramiento de los productos y servicios ofrecidos a sus clientes.

3. Las instituciones Financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, tiene la necesidad de adaptar su gestión hacia una cultura de prevención y administración de los diferentes riesgos a los que se enfrenta su giro del negocio, entre ellos principalmente el riesgo operacional y además deben velar por la continuidad del negocio para brindar una mayor estabilidad a sus clientes.

4. La Administración del riesgo tecnológico es un aspecto fundamental dentro de la gestión de riesgo operacional y es una de las responsabilidades y desafíos más importantes a las cuales se enfrenta las instituciones Financieras no supervisadas por la Superintendencia del Sistema

Financiero de El Salvador en la zona Occidental, debido al uso de recursos humanos, financieros y tecnológicos.

5. La responsabilidad de las instituciones financieras no reguladas por la Superintendencia del Sistema Financiero de El Salvador, va más allá de limitarse a hacerse cargo de controlar los riesgos que dependen de sus acciones, ya que aunque los eventos de riesgo sean generados por terceros, de igual manera deben intentar disminuir las consecuencias del riesgo. Cuando uno no puede anticiparse a los hechos, lo profesional es preparar planes de acción para mitigar los incidentes y establecer soluciones o controles alternativos.

6. Toda institución financiera ya sea de la zona occidental o de cualquier parte del país, aunque no esté obligada a ser supervisada por la Superintendencia del Sistema Financiero de El Salvador, tiene la necesidad de crear una cultura de prevención y administración de riesgos no solo operacional sino en todos los que se enfrenta en su giro de negocio; estos pueden ser de mercado, de liquidez y operacional.

7. El estudio del riesgo operacional es cada vez más imprescindible en las instituciones y cada empresa debería buscar la manera de implementar el mismo por la gran ayuda que brinda para la detección de riesgos asociados con Procesos, Personas, Tecnología de la Información, y Eventos Externos a su operatividad normal.

5.2 Recomendaciones

1. Las instituciones Financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, deben estar conscientes sobre la necesidad de incorporar a sus procesos de negocio la administración del riesgo operacional, como una oportunidad de lograr objetivos institucionales, agregar valor a sus líneas de negocio y estructura organizacional, alcanzar una ventaja competitiva y garantizar en forma sustentable su desarrollo administrativo, operativo, financiero y tecnológico.

2. Las instituciones Financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, deben adoptar una cultura de continuidad del negocio, para esto deben adaptar sus lineamientos, políticas y procedimientos de control interno hacia la administración de la continuidad de sus procesos, dentro de ellos la tecnología de la información ya que estos últimos son la base sobre la que se desarrollan sus operaciones y cuya interrupción puede generar pérdidas importantes a nivel financiero y reputacional.

3. La diferencia entre tener y no tener un plan de continuidad del negocio en una institución Financiera no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, es que la institución pueda desaparecer en caso de un incidente grave que perjudique sus principales procesos, por ello se considera necesario desarrollar un plan de continuidad para estar preparados ante cualquier incidente.

4. Las instituciones financieras no supervisadas por la Superintendencia del Sistema Financiero de El Salvador en la zona Occidental, deben estar conscientes sobre las necesidades de

incorporar a sus negocios la administración del riesgo operacional y de control interno, para resolver sus debilidades con respecto a riesgo como oportunidad para el logro de objetivos y metas institucionales. Sin embargo estas no tienen tantos recursos disponibles para la inversión en todos los controles relativos a riesgo operacional. En esos casos es más importante realizar anticipadamente una evaluación de cuál serían los posibles riesgos a los que están o pueden estar expuestos de manera que permita identificar los de mayor gravedad para concentrarse en los mismos y decidir el tratamiento que se dará a los otros riesgos; eso involucra realizar un adecuado análisis costo-beneficio.

Resumen ejecutivo

Informe de evaluación de riesgo operacional.

Riesgo general: Alto.

Las actividades desarrolladas dentro del plan de mitigación de riesgo operacional tienen como finalidad servir de apoyo en el proceso de identificación, medición, control, mitigación y comunicación del riesgo operacional, en las actividades que ejecuta la institución, presentando propuestas de solución a los riesgos identificados.

A continuación se muestra el resumen de las áreas revisadas y los resultados obtenidos:

Resumen de actividades analizadas

RIESGO	ÁREAS REVISADAS
OPERACIONAL	PROCESOS
	PERSONAS
	TECNOLOGÍA DE LA INFORMACIÓN
	EVENTOS EXTERNOS

Recomendaciones generales:

- Es necesario establecer políticas de proceso, incorporación, permanencia y desvinculación del personal a la institución.
- Establecer código de acceso a información de acuerdo a la posición dentro de la institución.
- Mejorar los procedimientos de caja para evitar robos de dinero y documentos mercantiles.

- Verificar los fondos de los asociados con el fin de evaluar que sean lícitos.
- Elaborar manuales y reglamentos relacionados con la tecnología de la información, que contengan normas, principios y lineamientos que establezcan responsabilidades y procedimientos para las operaciones.
- Contar con planes de continuidad del negocio de incidentes identificados para estar preparados en caso de eventos externos.

Bibliografía

- **Libros**:

1. Siklos, Pierre ,Money, Banking, and Financial Institutions: Canada in the Global Environment. Toronto: McGraw-Hill Ryerson, 2001.

2. Robert E. Wright and Vincenzo Quadrini. Money and Banking: Chapter 2 Section 5: Financial Intermediaries.

3. Gumersindo Ruiz, José Ignacio Jiménez y Juan José Torres, La gestión del riesgo financiero, 2000.

4. Baez Bruno, Matriz de Riesgo Operacional, 2010.

5. Hernández Sampieri, Roberto / Fernández Collado, Carlos / Baptista Lucio, Pilar., Metodología de la investigación, 6ta. Edición.

- **Sitios web**

1. Superintendencia del Sistema Financiero de El Salvador: http://www.ssf.gob.sv/index.php/servicios-14309/enlinea/ofertas-empleo/211-temas/entidades-no-supervisadas

2. FEDECREDITO: https://www.fedecredito.com.sv/qsomos.php

3. FEDECACES: http://www.fedecaces.com/site/nosotros

4. El Consejo de Estabilidad Financiera: http://www.fsb.org/about/contact.htm

5. Acuerdos de Basilea II: http://www.bis.org.

- **Leyes y Normas**

1. Ley de creación del Instituto Salvadoreño de Fomento Cooperativo.

2. Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito.

3. Normas para la gestión integral de riesgos de las entidades financieras, NPB4-47, 2012.

4. Normas para la gestión del riesgo operacional de las entidades financieras, NPB4-50.

5. Normas técnicas para la gestión de la continuidad del negocio, Banco Central de Reserva de El Salvador, 2015.

- **Artículos, monografías y otros**

1. Elder Salinas Zhunio y Esteban Gaona Troya, Elaboración de un plan de mitigación de riesgo operacional, Ecuador, 2012.

2. Carlos Palma Rodríguez, ¿Cómo construir una matriz de riesgo operativo?, Costa Rica, 2011.

3. Javier Veliz Madinya, Plan de mitigación de riesgo de los procesos, Ecuador. 2013.

4. Laura del Pinto, Guía de desarrollo de plan de continuidad del negocio.

5. Alfonso de Lara Haro, Medición y control de riesgos financieros, 2003.

Anexos

Anexo 1 Análisis del impacto BIA

ANALISIS DEL IMPACTO BIA			
		FECHA:	

NOMBRE DE LA DEPENDENCIA		NOMBRE DEL AREA	
GERENTE DEPENDENCIA		JEFE DE AREA	
CARGO		CARGO	

PROCEDIMIENTO #	NOMBRE DEL PROCEDIMIENTO	VALORACION VIA		
		CALIFICACION BIA	TIEMPO OBJETIVO DE RECUPERACION	VALOR DEL BIA
PROCEDIMIENTO 1				
PROCEDIMIENTO 2				
PROCEDIMIENTO 3				
PROCEDIMIENTO 4				
PROCEDIMIENTO 5				
PROCEDIMIENTO 6				
PROCEDIMIENTO 7				
PROCEDIMIENTO 8				
PROCEDIMIENTO 9				
PROCEDIMIENTO 10				

LIDER DEL PCN		OBSERVACIONES:
CARGO LIDER DEL PCN		

Anexo 2 Cuestionario BIA

CUESTONARIO BIA	
NOMBRE DEL PROCEDIMIENTO	

COMPRUEBE DEPENDENCIA PARA SER LLENADO POR PCN	¿Este procedimiento proporciona información crítica para cualquier otro procedimiento (Por favor, indique "Sí" o "No")
	Por favor indique el nombre del procedimiento si la respuesta anterior es Sí
	Proporcione la calificación BIA de acuerdo al procedimiento mencionado anteriormente.

IMPACTOS PARA SER ANALISADOS POR EL AREA DE NEGOCIO/APOYO	**REGULATORIO/LEGAL**
	Durante una interrupción de las operaciones normales del procedimiento, describa el plazo en el cual las sanciones por el incumplimiento podría superar el 20% de las utilidades
	Describa el periodo de tiempo dentro del cual el resultado de incumplimiento daría lugar a Penalizaciones, sanciones, multas y/o Investigación contra del Institucion
	FINANCIERO
	Durante una interrupción de las operaciones normales del procedimiento, describir el período en el que:
	La institucion pueda perder una ganancia de mas del 20%
	La institucion dejaría de percibir ingresos, a través de préstamos o productos que supera el 20%
	SERVICIO A CLIENTE EXTERNO
	¿Cuál es el tiempo máximo en que el procedimiento debe ser recuperado sin causar un impacto significativo al Instituto o al Servicio al Cliente Externo?
	Número de clientes externos afectados diariamente
	REPUTACIONAL
	Evalue el efecto del impacto reputacional en cuanto a las opiniones de los clientes, sectores educativo y financiero y/o el publico en general
	PROCEDIMIENTOS
	¿Cuál sería el impacto en otros procedimientos o áreas?
	PROVEEDORES
	Describa la importancia de las actividades de sus proveedores externos en sus procedimientos.
	PROVEEDORES CRITICOS
	El procedimiento tiene proveedores críticos.

	Clasificación Final Derivada BIA
	Tiempo Objetivo de Recuperación (RTO)
	Valor del BIA

Describa el tiempo máximo tolerable que está dispuesto a perder de información de su procedimiento ante una interrupción en los sistemas de información

Anexo 3 Reporte de incidentes de contingencia

REPORTE DE INCIDENTES DE CONTINGENCIA

INFORMACION DE IDENTIFICACION			
FECHA DEL INCIDENTE		HORA DE OCURRENCIA	
DURACION DEL INCIDENTE		PROCESO AFECTADO	
NOMBRE DEL AREA		LUGAR DONDE SE PRESENTO EL INCIDENTE	

DESCRIPCION DEL RIESGO

DESCRIPCION DEL INCIDENTE (PROBLEMA OCASIONADO)

CAUSAS DEL INCIDENTE

MEDIDAS DE CONTINGENCIA ADOPTADAS		
ACCION	PARTICIPANTES	
	NOMBRE	CARGO

RETORNO A LA OPERACION NORMAL

LECCIONES APRENDIDAS

ELABORADO POR		REVISADO POR	
NOMBRE		NOMBRE	
FIRMA		FIRMA	