UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSTGRADO

MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

Autoras:
Ing. FÁTIMA BEATRIZ VÁSQUEZ VELÁSQUEZ
Ing. JULIANA DEL PILAR ALVA ZAPATA

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

Chiclayo, Perú
2018

MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

POR

FÁTIMA BEATRIZ VÁSQUEZ VELÁSQUEZ
JULIANA DEL PILAR ALVA ZAPATA

Tesis presentada a la Escuela de Postgrado de la Universidad Católica Santo Toribio de Mogrovejo, para optar el Grado Académico de
MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADO POR

_____

Mtro. Gregorio Manuel León Tenorio

Presidente de Jurado

_____

Mtro. Ricardo David Imán Espinoza

Secretario de Jurado

_____

Mtro. María Ysabel Arangurí García

Vocal/Asesor de Jurado

CHICLAYO, setiembre 2018

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La gestión de riesgos de tecnologías de información (TI), elemento importante del gobierno de TI, no ha sido considerada en épocas anteriores, sin embargo hoy es muy apreciada y genera el interés tanto de los ejecutivos de negocio como de TI, para mitigar los riesgos que se originan a partir del uso de las tecnologías de la información sobre todo en un sector como el microfinanciero.

En esta investigación se presenta una propuesta de solución frente a los problemas que actualmente existen en las microfinancieras, las cuales muestran deficiencias para la gestión de riesgos de TI que podrían afectar a la continuidad del negocio, denigrar de la imagen institucional y generar pérdidas considerables de dinero y de clientes. Este estudio aplica el análisis de la situación actual de la gestión de riesgos de TI del sector microfinanciero, que incluye la revisión de la documentación relacionada y las normativas que deben cumplir, aplicando las metodologías y estándares de gestión de riesgos de TI, que hacen posible la propuesta del modelo adaptado a este contexto.

Se aplicó un estudio descriptivo - no experimental a tres microfinancieras con sede central en la región Lambayeque, luego a través del juicio de expertos y la aplicación de un caso de estudio se logra contrastar la hipótesis planteada. Finalmente, esta investigación quiere demostrar que con la implementación del modelo de gestión de riesgos de TI se contribuye a la continuidad del negocio de microfinancieras de la región Lambayeque.

Palabras clave: gestión de riesgos de TI, gobierno de TI, microfinancieras de la región Lambayeque.

ABSTRACT

Information technology (IT) risk management, an important element of IT governance, has not been considered in previous times, however today it is highly appreciated and generates the interest of both business executives and IT to mitigate risks that originate from the use of information technologies especially in a sector such as microfinance.

This research presents a proposed solution to the problems that currently exist in microfinance institutions, which show deficiencies in the management of IT risks that could affect business continuity, denigrate the institutional image and generate considerable losses of money and customers. This study applies the analysis of the current situation of the IT risk management of the microfinance sector, which includes the review of the related documentation and the regulations that must be complied with, applying IT risk management methodologies and standards, which make possible the proposal of the model adapted to this context.

A descriptive - non-experimental study was applied to three microfinance institutions with headquarters in the Lambayeque region, then through the judgment of experts and the application of a case study, the hypothesis proposed was tested. Finally, this research aims to demonstrate that the implementation of the IT risk management model contributes to the continuity of the microfinance business in the Lambayeque region.

Keywords: IT risk management, IT governance, microfinance of the Lambayeque region.

INTRODUCCIÓN

El trabajo de investigación presentado, analiza la situación actual de la gestión de riesgos de TI, donde el riesgo forma parte inherente al momento de hacer negocios debido a los cambios e incertidumbres propios de la actividad empresarial, por lo cual las empresas ponen sus esfuerzos para encontrar la forma más adecuada de absolver y mitigar los riesgos que pueden encontrarse en sus procesos e infraestructura. Las instituciones en las que se enfoca este trabajo están vinculadas al sector microfinanciero, en el cual la TI toma un papel importante, siendo que requieren de la misma para dar un servicio eficiente que permita atender los requerimientos financieros de los clientes.

Analizando el ámbito internacional, existen algunas empresas que han vivido experiencias realmente complejas demostrando la necesidad de hacer gestión de riesgos de TI: el caso de "Comair" una empresa subsidiaria de "Delta Air Lines", la cual experimentó un incidente con su sistema de planeación de horarios para tripulaciones. Este sistema, de misión crítica, para la operación del negocio, dejó de funcionar un 24 de diciembre y causó una interrupción total de sus vuelos, dejando pérdidas equivalentes a las utilidades operativas de todo un trimestre. Otro caso es el de "Card Systems Solutions Inc.", una procesadora de tarjetas de crédito; la cual a mediados del 2005 reportó que individuos desconocidos

obtuvieron acceso a las transacciones de 40 millones de tarjetahabientes. Visa y Mastercard, clientes de Card Systems, cancelaron su negocio con la empresa, que luego fue vendida (Ricardo Gómez 2010). En los casos expuestos se puede notar que la mayoría de los ejecutivos de TI prefieren evitar la gestión de riesgos; lo cual genera pérdidas a la organización porque no están preparadas para asumirlo, además cuando se adopta un enfoque demasiado estricto sobre los riesgos de TI pasando por alto los riesgos para el negocio y los posibles beneficios, limitan sus oportunidades de impulsar la ventaja económica y operativa en sus empresas (IBM 2008).

Otro punto a tener en cuenta es, que los riesgos de TI hasta ahora se han considerado como responsabilidad única del departamento de TI y no como un riesgo estratégico de negocios que requiere la atención de toda la compañía, sin tener en cuenta que a medida que el uso generalizado de la tecnología de información y sus herramientas continúan en aumento, afectan prácticamente todos los aspectos de la función empresarial y cada vez es más claro que la administración de estos riesgos trata más sobre la administración de riesgos para todo el negocio (Young 2010).

Según un informe de riesgos realizada por Ernst & Young en el 2010, existen 10 riesgos más relevantes para bancos y las empresas tecnológicas, en donde se encuentra que la mayoría de los riesgos del negocio tienen un fuerte vínculo con los riesgos de TI, entre ellas el riesgo reglamentario y el riesgo operativo. Las instituciones financieras debido a la importancia de su rol en el desarrollo económico de un país, están sujetas a una estricta regulación. Ejemplos de estas son: los marcos Basilea I y II, la Ley de Sarbanes – Oxley (originado debido al caso Enron), Ley 510 (S. 2014). En Colombia, la ley 510 de 1999, en Argentina y Perú, el marco Basilea II son los marcos utilizados. En el Perú, el órgano encargado de supervisar a las entidades financieras es la Superintendencia de Banca, Seguros y AFP (SBS). Todas las instituciones supervisadas por la SBS, se encuentran inmersas en el cumplimiento de las normativas emitidas por este ente

regulador, y entre los riesgos que son evaluados como parte del desarrollo de sus actividades se encuentra el riesgo operacional, el cual es otro componente de la gestión de riesgos según BASILEA II, (Celi 2015). Uno de los aspectos a evaluar por el riesgo operacional es el factor del riesgo de TI. Según un informe realizado por Deloitte, en el año 2014, se indicaba que el Perú era el segundo país en Latinoamérica en sufrir fraudes internos, originados por las brechas de seguridad interna. Ante esto, la SBS plantea en el reglamento para la gestión del riesgo operacional que las empresas deben gestionar los riesgos asociados a la tecnología de información, 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, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

En la región Lambayeque, existe un número significativo de instituciones microfinancieras operando. Todas ellas cuentan con un área de riesgos que analiza los distintos tipos de riesgos, según lo requerido por la SBS, pero si se evalúa a detalle, se puede observar que no se presta la debida importancia a los riesgos tecnológicos, dado que aún son empresas pequeñas y jóvenes, trayendo consigo pérdidas para la organización. Esta situación se evidencia en un caso ocurrido en el 2011 en una de las microfinancieras en estudio, quién sufrió pérdidas que sumaban los S/100,000.00 por un error que se originó al realizar un pase a producción para la implementación de una nueva campaña. A nivel de hardware, en el año 2016, otra de las microfinancieras en estudio sufrió grandes pérdidas debido a que su servidor principal colapsó y no se logró levantar a tiempo el servidor de respaldo por falta de pruebas del plan de continuidad. Estas situaciones de riesgo para las organizaciones, pueden evitarse realizando una adecuada gestión de riesgos que de soporte a la continuidad del negocio.

Bajo el análisis de la situación problemática descrita, se formula la siguiente interrogante ¿De qué manera se puede contribuir en la continuidad del negocio de las microfinancieras, de la región Lambayeque? Para dar respuesta a esta interrogante se planteó la siguiente hipótesis: con la implementación del modelo de gestión de riesgos de TI se contribuye a la continuidad del negocio de microfinancieras de la región Lambayeque.

El objetivo general de esta investigación es, contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque, mediante el desarrollo de un modelo de Gestión de Riesgos de TI. Para lograr el cumplimiento este objetivo se han planteado los siguientes objetivos específicos: determinar la armonización de las metodologías, estándares y normas de gestión de riesgos de TI; analizar el impacto de negocio para identificar los procesos esenciales que contribuyen a la continuidad del negocio; configurar la estructura del esquema estándar para la formulación de planes de acción de TI y validar el modelo propuesto en cuanto a la utilidad para las microfinacieras.

Esta investigación se justifica desde el aspecto legal en el sector microfinanciero, porque resulta importante gestionar adecuadamente los riesgos ya que está de por medio el cumplimiento normativo establecido por la SBS, quien mediante la circular G-140-2009, obliga a las empresas financieras a establecer criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información.

Se justifica también esta investigación desde el punto de vista económico, ya que es importante considerar que una adecuada gestión de riesgos, permite asignar de manera preventiva los recursos económicos suficientes, para responder frente a los riesgos de TI identificados. Relacionado al aspecto tecnológico, la investigación establecerá un modelo de gestión de riesgos basado en estándares, metodologías y herramientas que proporcionan las guías necesarias para reducir el nivel de vulnerabilidad

que tienen los activos ante la materialización de una amenaza, proponiendo una adaptabilidad al contexto financiero que facilite su aplicabilidad en la organización con respecto a las TI que la soportan. Además se considera una justificación desde el aspecto social, porque mejora la gestión de riesgos de TI que impacta positivamente en el clima organizacional, ya que se manejarán los riesgos de manera planificada y eso se reflejará dentro y fuera de la organización creando una correcta imagen empresarial.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1 Antecedentes

Para dar un sustento a la propuesta aquí planteada, se ha considerado fundamentar a través de los antecedentes seleccionados como investigaciones previas relacionados con el tema.

Según Álvarez (2013), en su investigación propone una metodología para el análisis de riesgos en las universidades de Barquisimeto Estado Lara, que propone como objetivo mitigar los riesgos, para aumentar la productividad operacional y mantener disponibles los servicios de tecnología que ofrecen a su comunidad estudiantil. El procedimiento que el autor consideró plantea un diagnóstico en una muestra de universidades locales, luego se hace comparación metodológica para identificar criterios comunes a las mismas y por último el diseño de la propuesta, que plantea finalmente, la metodología propuesta como resultado de la tesis que genera el aporte de la secuencia lógica de la cual hizo uso para el desarrollo de la presente tesis.

Yépez (2011), brinda un aporte cualitativo y técnico, sobre las debilidades detectadas a través de la identificación de puntos vulnerables en las tecnologías de información y aquellas que hacen

referencia específicamente a la gestión tecnológica como tal, que incrementa actualmente el riesgo operativo en las instituciones financieras, utilizando como guía de trabajo un enfoque de riesgos conforme lo requiere la norma en la legislación ecuatoriana. De este antecedente se rescató la importancia que le dan a los puntos vulnerables en las TI que no están solo relacionadas a la seguridad de la información sino que también se centran en la continuidad del negocio.

Crespo (2013), expone un estudio de las principales metodologías, normas y marcos de trabajo existentes en el campo de la auditoría de sistemas de información. Su investigación se centra en el análisis de riesgos, primero el autor plantea un estudio teórico sobre el concepto de análisis y gestión del riesgo, para a continuación llevar a cabo un estudio de las diferentes metodologías y estándares existentes en el mercado. Finalmente, se expone una metodología propia para llevar a cabo una auditoría informática utilizando un análisis de riesgos. Hoy en día las auditorias en el sistema financiero son constantes ya que son entes frecuentemente regulados por el gobierno y el analizar los riesgos de una manera más profunda, durante una auditoría, puede ser de gran ayuda de tal manera que se logra un mejor control de resultados a corto plazo.

Mogollón (2015), expone una comparación de algunas de las metodologías disponibles y usadas actualmente, tales como OCTAVE, MAGERIT, MEHARI; con el fin de conocer las características, fases, ventajas y desventajas asociadas. De esta forma, escoger la que mejor se adapte a las necesidades de la empresa u organización, con esto se busca el mayor éxito posible a la hora de su implementación. Se ha creído conveniente citar este artículo porque explica de una manera entendible y resumida las diferencias más resaltantes que existen entre las metodologías de gestión de riesgos.

Celi (2015), propone un modelo para la gestión de riesgos operativos relacionados con las tecnologías de información como parte de un sistema de gestión de la seguridad de la información, desde una perspectiva que integra técnicas cuantitativas y cualitativas. La importancia de este antecedente es que el estudio está dirigido para empresas microfinancieras de la región Lambayeque, que es el mismo objeto de estudio de esta investigación, lo que permite conocer más a detalle las normas y los criterios considerados para este sector.

Gómez y otros autores (2010), muestran qué tipo de estándares y normas se deben considerar al realizar un análisis de riesgos, posteriormente explican cómo utilizar una metodología y cómo articularla en el proceso de gobernabilidad de TI para desarrollar en forma exitosa este tipo de iniciativas.

1.2 Base Teórico Conceptual

En este apartado se hará referencia de cada uno de los conceptos se han sido aplicados en el desarrollo de la presente tesis que define el sustento teórico del método propuesto.

1.2.1 Gobierno de TI

Antes de poder pasar a una definición más formal de gobierno de TI, es necesario comprender a que se refiere el gobierno en la empresa. Según la real academia española, gobernanza se define como "*arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía".* Gobierno es el "*elemento que resulta de organizar a las personas con el propósito de alcanzar los objetivos de la comunidad, de entre los cuales destacan la protección del territorio, la seguridad de sus habitantes y su desarrollo integral"* (Muñoz 2011).

El gobierno de TI, se define como la estructura de relaciones y procesos para dirigir, así como controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos.

El gobierno de TI integra e institucionaliza las buenas prácticas de la empresa, para garantizar que TI dé soporte a los objetivos del negocio. Facilita que la empresa aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas (Muñoz 2011).

El gobierno de TI es una pieza clave dentro de este proceso, para asegurar la pertinencia y el éxito de las decisiones que se tomen respecto a los riesgos, dado que para tomar la decisión sobre qué tipo de estrategia utilizar, se hace necesario realizar un análisis de cada riesgo para conocer y cuantificar el impacto si el riesgo se materializa, así como su probabilidad de ocurrencia. Ahora, estas decisiones de qué hacer con los riesgos deben estar alineadas con el esquema estratégico de la organización (Gómez, y otros 2010).

Dada la importancia del concepto de gobierno de TI, como un aspecto de apoyo en la implementación de cualquier cambio propuesto, se considera importante lo indicado por Fernández (2009), en cuanto a las responsabilidades y prácticas ejecutadas por la junta directiva, como por la administración ejecutiva con el fin de proveer dirección estratégica, que garantice el alcance de los objetivos propuestos como pieza clave dentro de este proceso.

Uno de los marcos de gobierno de TI usados es COBIT 5 (Control Objectives for Information and related Technology) el cual proporciona un marco integral que ayuda a las organizaciones a lograr su metas y entregar valor mediante un gobierno y una

administración efectivos de la TI de la organización. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5, permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público (ISACA 2012). Este marco se usará como guía, para el diseño del método propuesto para microfinancieras.

COBIT 5 para riesgos, se basa en el marco COBIT 5, centrándose en el riesgo y proporcionando una orientación más detallada y práctica a los profesionales de riesgo y otras partes interesadas en cualquier nivel de la empresa. Los procesos principales del gobierno y la gestión de riesgos están descritos en los procesos de COBIT 5: EDM03 (Asegurar la optimización del riesgo) y APO12 (Gestionar el riesgo). Estos procesos comprenden las actividades principales de la función de riesgos y brindan soporte a la empresa en la obtención de los objetivos corporativos y del valor para las partes interesadas, en tanto se optimizan los recursos y los riesgos. (ISACA 2013).

En COBIT 5 para riesgos, el proceso APO12 conjuntamente con los catalizadores (o habilitadores) permiten a la empresa construir, ejecutar y supervisar una eficiente y efectiva función de gestión de riesgos. En la siguiente figura se muestran los catalizadores y los subprocesos que se desarrollan en el proceso APO12.

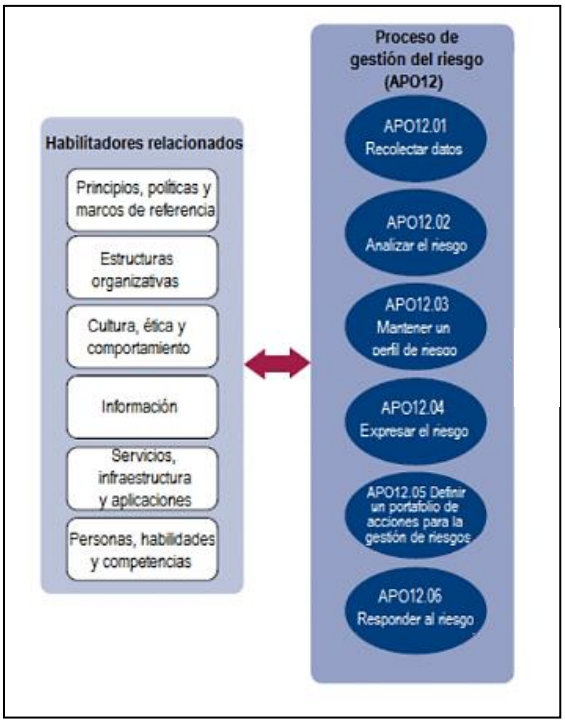


Figura 1. Proceso de Gestión del riesgo y Catalizadores
Fuente: Adaptado de (ISACA 2013)

COBIT 5 para riesgos, se usa para el análisis de contexto interno o externo del método propuesto. También se consideran conceptos para la valoración de activos y el tratamiento de riesgos.

1.2.2 Gestión de riesgos

La SBS, en el reglamento de gestión de riesgos (2008) la define como "*definición de la estrategia de una empresa, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos*".

La gestión de riesgos utiliza los resultados del análisis de riesgos y ayuda a seleccionar y establecer las medidas de seguridad apropiadas para controlar los riesgos identificados.

En la siguiente figura, se pueden ver los factores que influyen para reconocer las situaciones de riesgos de una organización, a través de la identificación de las amenazas y vulnerabilidades y reconociendo situaciones críticas, a estas actividades en conjunto forman el análisis de riesgo, el cual sirve de base para la gestión de riesgos.

Figura 2. Relación de Concepto de Riesgos

Fuente: (Crespo Rin 2013)

La gestión de riesgos, se considera importante en esta investigación, porque resulta primordial tener claro desde una visión global la gestión de riesgos de tal manera que se pueda diseñar el modelo con los principios que se contemplan en esta práctica.

En este ámbito es necesario definir lo que significa la palabra riesgo. Haciendo mención a la definición que hace la real academia española de la lengua; en su primera acepción lo define como "*contingencia o proximidad de un daño*" y en la segunda como

"*cada una de las contingencias que pueden ser objeto de un contrato de seguro*".

En el lado financiero, la SBS en el reglamento de la gestión integral del riesgo (2008) define al riesgo como "*la condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa".*

Una de las definiciones de ISACA es "*evento que, de ocurrir, afecta negativamente el logro de un cierto objetivo, pudiendo impedir la creación de valor para la organización o erosionar el valor existente* (Guirado 2015).

MAGERIT define riesgo como, *"la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización"* (Crespo Rin 2013).

Por otro lado, la norma ISO/IEC 27002:2005 define el riesgo como la "*combinación de la probabilidad de un evento y sus consecuencias; llamándose a esto riesgo basado en escenarios o riesgo basado en situaciones, conocido también como modelo de riesgo dinámico donde el tiempo juega un rol y como resultado, diferentes fases del escenario del riesgo en cuestión resultan en diferentes tipos de acción"* (Alvarez Sosa 2013).

En esta investigación se toma en cuenta el concepto que indica, que el riesgo ocurre cuando una amenaza se materializa sobre uno o más activos causando daños y que estos eventos al ocurrir, afectan negativamente el logro de los objetivos estratégicos de la organización. Es por ello que se considera que los activos son los puntos más críticos de una empresa, por lo tanto, deben reconocerse las amenazas para así poder definir los posibles

riesgos que puedan afectarlos, realizar una correcta gestión de los riesgos y lograr la continuidad del negocio, de tal manera que no se vea afectado el logro de ciertos objetivos del negocio que proporcionan valor a la organización.

La SBS en el reglamento para la gestión de riesgos (2008) lista diversos tipos de riesgos:

- **Riesgo crediticio:** posibilidad de pérdidas por la imposibilidad o falta de voluntad de los deudores o contrapartes.
- **Riesgo estratégico:** posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles.
- **Riesgo de liquidez:** posibilidad de pérdidas por incumplir con los requerimientos de financiamiento y de aplicación de fondos que surgen de los descalces de flujos de efectivo.
- **Riesgo de mercado:** La posibilidad de pérdidas en posiciones dentro y fuera de balance derivadas de fluctuaciones en los precios de mercado.
- **Riesgo operacional:** la posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.
- **Riesgo de seguro:** la posibilidad de pérdidas por las 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.
- **Riesgo de reputación:** la posibilidad de pérdidas por la disminución en la confianza en la integridad de

la institución que surge cuando el buen nombre de la empresa es afectado.

1.2.3 Gestión de riesgos de TI

Luego de definir los conceptos de la gestión de riesgos en general, se considera conveniente previamente conceptualizar el análisis de riesgo vinculado a TI.

MAGERIT lo define como "*proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema"*. En coordinación con los objetivos, estrategia y política de la organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección. Al conjunto de estas actividades se le denomina proceso de gestión de riesgos (Gobierno de España 2012).

El análisis y gestión del riesgo tecnológico consiste en identificar el nivel de seguridad que requiere la organización en materia de información, aportando elementos claros para la alta dirección, para aprobar iniciativas, recursos y presupuestos enfocados a alcanzar los niveles aceptables de riesgo para la organización (Vásquez 2013).

Otras definiciones que toma en cuenta MAGERIT dentro del análisis de riesgo se exponen a continuación:

- **Activos:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (Gobierno de España 2012).

- **Amenazas:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (Gobierno de España 2012).

- **Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza (Gobierno de España 2012).

- **Probabilidad:** Según el diccionario de la Real Academia Española de la lengua, sería la razón entre el número de casos favorables y el número de casos posibles. Se refiere al estudio cuantitativo y/o cualitativo del número de veces que la amenaza puede materializarse (Gobierno de España 2012).

- **Vulnerabilidades:** Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial (Gobierno de España 2012).

1.1.4.1 Riesgo de TI

La SBS en el reglamento de riesgo operacional (2008) considera a las tecnologías de la información como uno de sus cuatro factores (procesos internos, personal, tecnologías de la información y eventos externos). Indica que las empresas deben gestionar los riesgos asociados a la tecnología de información, 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, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

ISACA, define el riesgo tecnológico como la "*probabilidad de pérdidas ante fallas de los sistemas de información"*. También considera la probabilidad de fraudes internos y externos a través de los sistemas de información. Involucra al riesgo legal y al riesgo de pérdida de reputación por fallas en la seguridad y por la no disponibilidad de los sistemas de información (Ibarra 2010).

Otra definición de ISACA es el riesgo de negocio asociado al uso, propiedad, operación, participación, influencia y adopción de las tecnologías de la información en la organización (Troitiño 2014).

La norma ISO/IEC 27005:2008 que sirve como guía para la gestión de riesgos de la seguridad de la información en los sistemas de gestión de seguridad de la información (SGSI) expresa, que el riesgo de seguridad de la información es el potencial de que una amenaza explote las vulnerabilidades de un activo o grupo de activos causando daño a la organización (Alvarez Sosa 2013).

Además se considera que, no se debe entender el riesgo tecnológico como un riesgo independiente, sino como un riesgo que está íntimamente vinculado al uso de la tecnología como parte del modelo de negocio.

La SBS en la circular G-140-2009, la información debe cumplir con los criterios de de los siguientes criterios:

- **Confidencialidad:** La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.

- **Integridad:** La información debe ser completa, exacta y válida.

- **Disponibilidad:** La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

Se consideran tres aspectos importantes para dimensionar el riesgo tecnológico: riesgo de nivel infraestructura tecnológico, que tiene que ver con redes, recursos hardware y accesos lógicos; riesgo lógico, en donde se considera al riesgo asociado al software, aplicaciones y datos; y por último el riesgo derivado al mal uso de las TI. Estos aspectos ayudaron a elaborar un mapa de riesgos para identificar las posibles causas.

Por último, la gestión del riesgo de TI involucra 3 aspectos: el riesgo tecnológico (sistemas, infraestructura, inversión de TI, entre otros), el riesgo de la información y el cumplimiento normativo; los cuales, si son controlados adecuadamente, logran asegurar la continuidad del negocio.

1.1.4.2 Metodologías para el análisis y gestión de riesgos de TI

En este punto se explican las metodologías que se han considerado más importantes para la investigación y sirvieron como base para crear un nuevo modelo de gestión de riesgos

adaptado a la problemática de las microfinancieras en la región de Lambayeque.

a. MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el consejo superior de administración electrónica. Inicialmente fue creado como un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Actualmente, se puede aplicar en diferentes tipos de empresas ya que su flexibilidad y facilidad de utilización lo permite. La primera versión se publicó en 1997. En 2006 se publica la versión 2.0. En octubre 2012, se ha publicado la versión 3.0.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza (Ochoa 2010).

En la siguiente imagen se muestra los elementos del proceso de análisis y gestión de riesgos según MAGERIT.

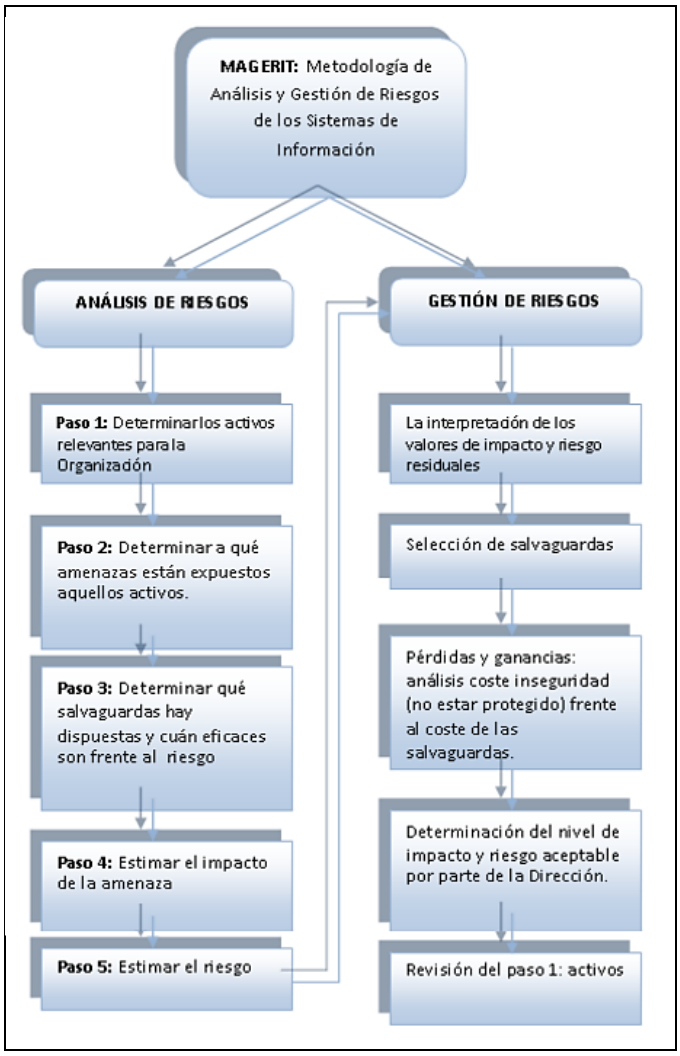


Figura 3. Elementos del proceso de análisis y gestión de riesgos

Fuente: (Crespo Rin 2013)

El análisis de riesgos, permite determinar qué tiene la organización y hacer una estimación sobre lo que puede pasar. En la gestión de riesgo, se interpreta lo analizado anteriormente y se identifican los mecanismos para el tratamiento de los riesgos.

La gestión de riesgos, permite organizar la defensa de manera concienzuda y prudente, posibilitando defensas para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

Como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Para la elaboración del método de gestión de riesgos propuesto, se han considerado de MAGERIT los conceptos sobre la identificación, clasificación y valoración de activos.

b. OCTAVE

Se centra en el estudio de riesgos organizacionales y se focaliza principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto como los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas, entre otros). De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa en el día a día. En OCTAVE, se considera que, con el fin de que una organización pueda cumplir su misión, los empleados a todo nivel necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos; para ello, es fundamental que en la evaluación estén directamente involucradas personas de diferentes niveles de la organización. (Gómez, y otros 2010)

Con relación a los activos, OCTAVE los clasifica en dos grandes grupos:

- Sistemas: Hardware. Software y Datos.
- Personas.

Cuando se aplica esta metodología se hace un trabajo conjunto con las diferentes áreas de la organización centrándose en las necesidades de seguridad y equilibrando los siguientes tres aspectos: riesgos operativos, prácticas de seguridad y tecnología.

El objetivo de OCTAVE va direccionado a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. En este caso la tecnología es examinada en proporción a las prácticas de seguridad, esto permite a las compañías realizar la toma de decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes afines a la información crítica.

En la siguiente figura, se esquematizan las 3 fases del desarrollo de OCTAVE.

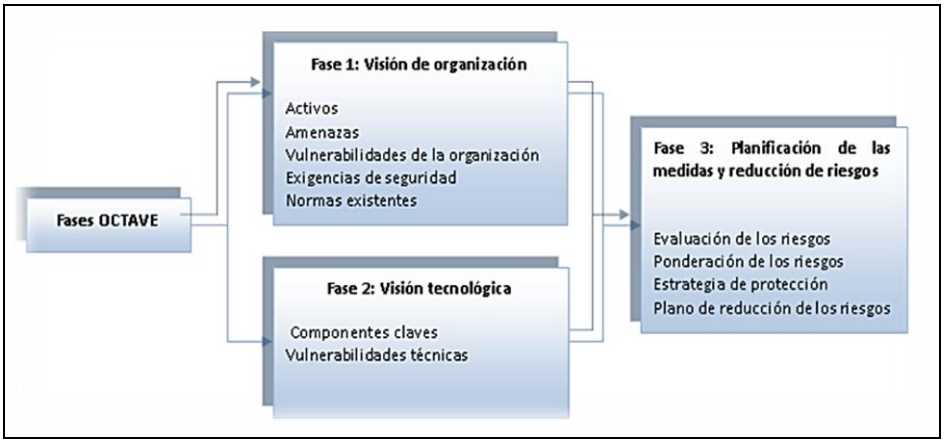


Figura 4. Fases de desarrollo de OCTAVE
Fuente: (Crespo Rin 2013)

En el método propuesto, se analiza lo establecido por OCTAVE referente a la clasificación y valoración de activos.

1.1.4.3 Estándar para la gestión de riesgos de TI

La norma internacional ISO/IEC 31000 es la norma internacional para la Gestión de Riesgos. Al proporcionar principios y Guía exhaustivos, esta norma ayuda a las organizaciones en sus análisis y evaluaciones de riesgos.

Según explicó Kevin W. Knight, todas las organizaciones, no importa si son grandes o pequeñas, se enfrentan a factores internos y externos que le quitan certeza a la posibilidad de alcanzar sus objetivos. Este efecto de falta de certeza es el riesgo y es inherente a todas las actividades (Castro 2010).

La ISO/IEC 31000:2009, establece una serie de principios que deben ser satisfechos para hacer una gestión eficaz del riesgo. Esta norma internacional, recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte (framework) cuyo objetivo es integral el proceso de gestión de riesgos en el gobierno corporativo de la organización, planificación y estrategia, gestión, procesos de información, políticas, valores y cultura (Castro 2010).

Las fases que la ISO/IEC 31000 identifica en el proceso de gestión de riesgos se muestran en la siguiente imagen.

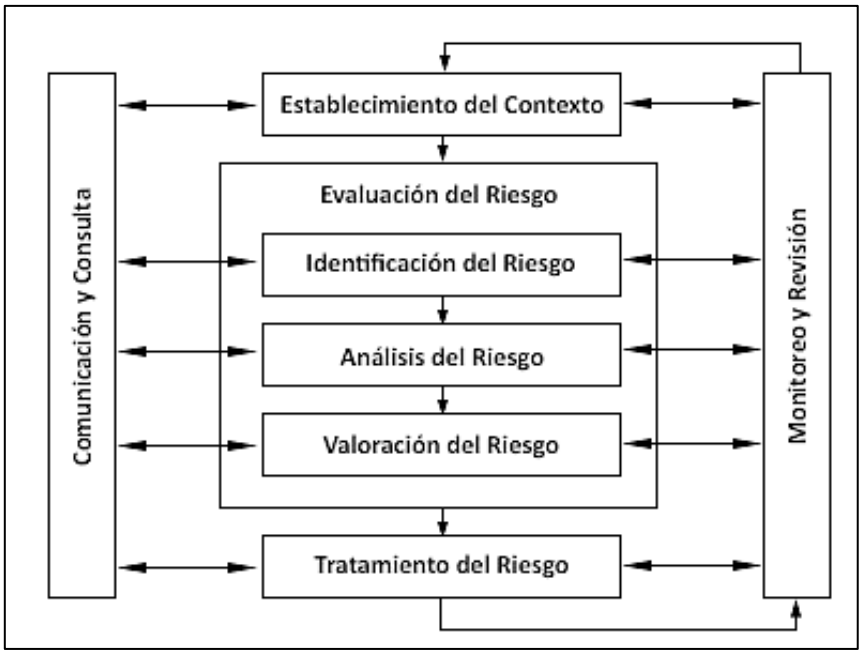


Figura 5. Proceso general de la gestión de riesgos
Fuente: (ISO/IEC 31000:2009)

- **Establecimiento del contexto**: Definir el alcance de la gestión de riesgo dentro de la organización.
- **Identificación del riesgo:** Identificar que, por qué y cómo pueden surgir elementos como base para el análisis posterior.
- **Análisis del riesgo:** Determinar los controles existentes y analizar los riesgos en términos de consecuencia y posibilidad en el contexto de esos controles.
- **Valoración del riesgo:** Comparar los niveles estimados de riesgo, contra los criterios pre-establecidos con el fin de realizar una priorización de la gestión.
- **Tratamiento del riesgo:** Desarrollar e implementar un plan de gestión para mitigar los riesgos identificados.
- **Monitoreo y revisión:** Consiste en verificar el desempeño del sistema de gestión de riesgo y los cambios que pudieran afectarlo.

- **Comunicación y consulta:** Desarrollar un proceso de comunicación efectiva que sirva de base para la toma de decisiones y para implementar los planes de acción que se requieran.

Se considera importe mencionar esta norma, porque este es el estándar base del método que se propone para la gestión de riesgos de TI en microfinancieras de la región Lambayeque.

1.2.4 Continuidad del negocio

Según la SBS en la circular G-139-2009, indica que la gestión de la continuidad del negocio es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Un sistema de gestión de continuidad del negocio (SGCN), es parte del sistema de gestión gerencial que establece, implementa, opera, evalúa, mantiene y mejora la continuidad del negocio. Un SGCN da confianza a terceros ya que ha identificado los procesos esenciales que soportan a los productos o servicios que se desean proteger de escenarios de amenazas producto del análisis del riesgo (Alexander 2012).

En el año 2012, la Organización Internacional para la Normalización (ISO) publicó el estándar Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos. Aplica el ciclo Plan-Do-Check-Act (PDCA) para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de su efectividad.

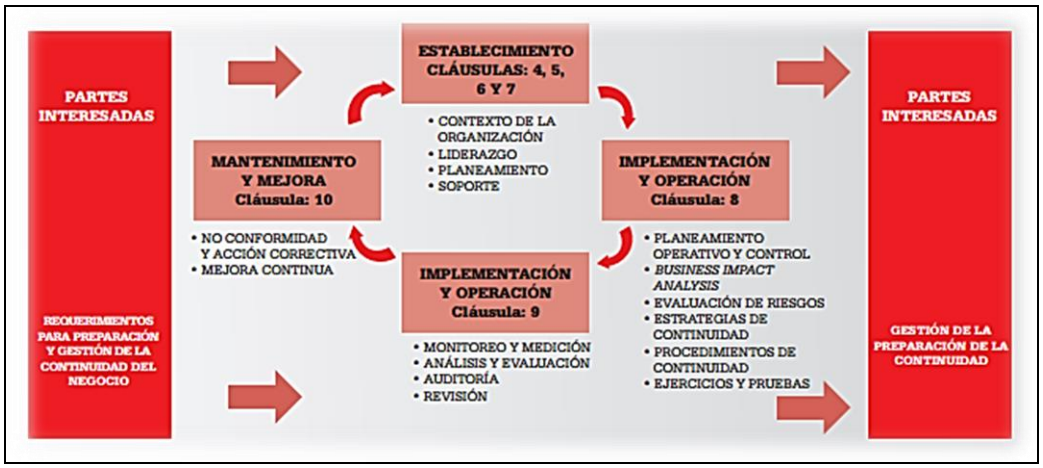


Figura 6. Ciclo PDCA aplicado al proceso de continuidad del negocio
Fuente: (Alexander 2012)

En la figura mostrada anteriormente, se puede apreciar como el SGCN toma insumos de las partes interesadas, requerimientos para la gestión de la continuidad, y a través de las necesarias acciones y procesos produce resultados de continuidad para cumplir con los requerimientos.

La norma internacional ISO/IEC 22301:2012 es una norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas. Especifica los requisitos necesarios para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar de forma continua el sistema de gestión para responder y recuperarse pronto de las interrupciones, en el momento en el que sucedan. Los requisitos que se especifican en la norma ISO/IEC 22301:2012 son genéricos y son aplicables a todas las empresas, no importa su tamaño, naturaleza o tipo. El grado de aplicación de los requisitos depende del ambiente operativo y de la complejidad de la empresa.

El objetivo general de esta investigación está orientado a contribuir a la continuidad del negocio, por tanto resulta importante tener claro los conceptos relacionados a este tema.

En el desarrollo de un plan de continuidad del negocio se ejecuta, una de las fases más importantes conocida como el análisis del impacto en el negocio (BIA), debido a que permite a las organizaciones estimar la magnitud del impacto operacional y financiero asociado a una interrupción. El BIA tiene dos objetivos principales; el primero de ellos consiste en proveer una base para identificar los procesos críticos para la operación de una organización. Una vez generado ese punto de partida, el segundo se refiere a la priorización de ese conjunto de procesos, siguiendo el criterio de cuanto mayor sea el impacto, mayor será la prioridad.

El BIA, está directamente relacionado con aquellos procesos que poseen un tiempo crítico para su operación, porque si bien todos los procesos sujetos a un tiempo crítico son de misión crítica, no todos los procesos de misión crítica están relacionados con un tiempo crítico para su ejecución.

De manera adicional, el desarrollo de este análisis permite estimar los recursos necesarios para los procesos identificados, de manera especial para aquellos que representan mayor sensibilidad con relación al tiempo y el impacto.

Para ello se define el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés), que es el período permitido para la recuperación de una función o recurso de negocio, a un nivel aceptable luego de una interrupción o desastre, y el Punto Objetivo de Recuperación (RPO) que describe la antigüedad máxima de los datos para su restauración, es decir, la tolerancia que el negocio puede permitir para operar con datos de respaldo, por lo que el

RPO estará en función de las actividades primordiales de una organización.

Resulta importante tener claro el concepto de BIA, porque en el método desarrollado se contempla una etapa que abarca el análisis del impacto del negocio, que es uno de los principios importantes en la continuidad del negocio.

1.2.5 Seguridad de la información

Según la ISO/IEC 27001 define a la seguridad de la información como "*preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad"* (Estándar Internacional ISO/IEC 27001 2005).

La norma ISO/IEC 27002:2005 define la seguridad de información como *"la protección de la información de un rango amplio de amenazas, para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales".*

Existen normas técnicas, que son documentos de aplicación voluntaria y tienen el carácter de acuerdos documentados que contienen los criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características.

En el ámbito internacional ISO e IEC tienen por objetivo favorecer el desarrollo de la normalización en el mundo, para facilitar los intercambios comerciales y las prestaciones de servicios entre los distintos países. Entre los documentos elaborados por ISO/IEC se encuentran las normas internacionales que son elaboradas por los

miembros participantes en un comité técnico, subcomité o grupo de trabajo y aprobada por votación entre todos los participantes; dentro de estas normas se encuentran las que proporcionan modelos para implementar la seguridad de la información en los SGSI de las organizaciones; entre ellas se encuentran las normas ISO/IEC 27001:2005, ISO/IEC 27002:2005 (Alvarez Sosa 2013).

La norma ISO/IEC 27005:2011, forma parte de la familia de ISO 27000 enfocada a la seguridad de la información, siendo un complemento a las normas ISO/IEC 27001 e ISO/IEC 27002, las cuales definen las necesidades de elaborar un análisis de riesgos pero no especifican directrices para ello.

Ésta norma proporciona un marco para la implementación de un enfoque de gestión de riesgos, ayudando a gestionar los riesgos en un sistema de gestión de seguridad de la información (SGSI). En la norma se describe el proceso de gestión de riesgos y apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005, tecnología de la información - técnicas de seguridad - sistemas de gestión de seguridad – requisitos.

La norma como tal, no proporciona ninguna metodología específica para la gestión de riesgos de seguridad, sino que aporta un enfoque genérico para la gestión de riesgos que debe apoyarse en metodologías específicas de análisis y gestión de riesgos; es aplicable a cualquier tipo de organización que quiera mejorar la gestión de sus riesgos en seguridad de la información.

La norma tiene el propósito de alinearse con ISO/IEC 31000:2009 con el fin de ayudar a las organizaciones que deseen gestionar sus riesgos de seguridad de la información de una manera similar a la forma de gestionar "otros" riesgos. ISO/IEC 27005:2011 ayudará a los usuarios en la implementación de ISO/IEC 27001, la norma de

sistemas de gestión de seguridad de la información, que se basa en un enfoque de gestión de riesgos.

La norma está estructurada en 12 cláusulas y 6 anexos que apoyan el desarrollo de cada una de las cláusulas.

El proceso de gestión de riesgos propiamente dicho se describe a partir de la cláusula 7 y que mencionan de forma general a continuación:

- **Cláusula 7.** Establecimiento del contexto, se definen los objetivos, el alcance y la organización para todo el proceso (políticas, enfoque)

- **Cláusula 8**. Valoración del riesgo, se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:
    - Identificación de riesgos
    - Estimación de riesgos
    - Evaluación de riesgos

- **Cláusula 9**. Tratamiento del riesgo, define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

- **Cláusula 10**. Aceptación del riesgo, se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado. Se debe tratar el riesgo residual.

- **Cláusula 11**. Comunicación del riesgo, todos los grupos de interés intercambian información sobre riesgos, esta comunicación debe hacerse durante todo el proceso.

- **Cláusula 12**. Monitoreo y Revisión del riesgo, el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos. Se realiza un monitoreo y evaluación continua.

La siguiente figura se muestra el proceso para la gestión de riesgos según el estándar ISO/IEC 27005:2011.

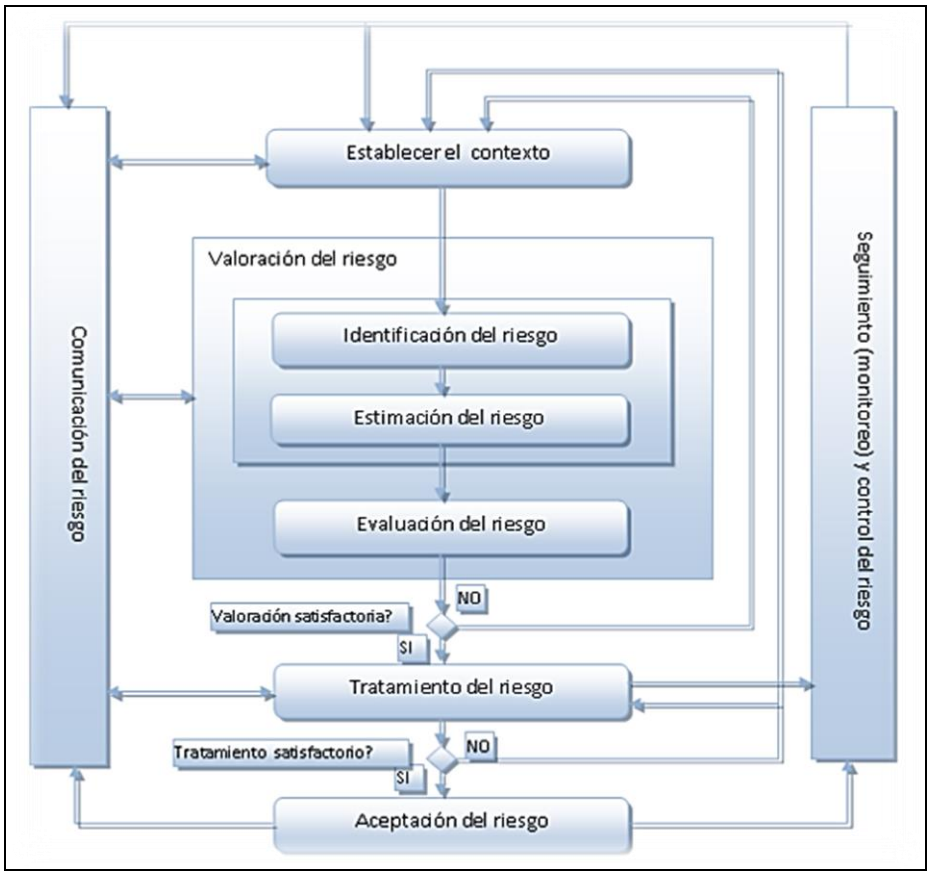


Figura 7. Proceso para la gestión de riesgos en ISO/IEC 27005
Fuente: (Crespo Rin 2013)

Se considera este estándar porque se toman conceptos sobre la identificación y clasificación de activos para el método

desarrollado. También se consideran las definiciones relacionadas a la valoración, tratamiento y monitoreo de riesgos.

1.2.6 Procesos en las microfinancieras

Para hacer posible el planteamiento de un método de gestión de riesgos, aplicado al sector microfinanciero, es necesario conocer los principales procesos que se desarrollan en este tipo de empresas.

Según Iparraguirre Vergara y Macedo (2011) se definen 8 macro procesos que pertenecen a los procesos operativos de toda entidad microfinanciera.

a. Inversiones

Es el proceso en el cual se vincularán recursos financieros propios, en proyectos de inversión, a la espera de la obtención de ganancias o dividendos. Cada proyecto de inversión y en general la cartera de Inversiones, debe contar con un análisis previo de factibilidad que tome en cuenta factores como el riesgo, rentabilidad, factores políticos, tiempos de retorno, etc.

b. Colocaciones

El proceso de Colocaciones, consta de planes de administración en la ubicación de los recursos de la microfinanciera, como créditos para determinados clientes. Esto abarca métodos de entrega de préstamos de dinero, bajo un análisis de la situación de clientes, es decir un estudio del historial y proyección de personas a las cuales prestar esos recursos.

c. Recuperaciones

El proceso de Recuperaciones se encarga de prevenir pérdida por créditos impagos otorgados a clientes que no cumplen con sus obligaciones con la microfinanciera. El proceso comprende desde la evaluación de los créditos no pagados hasta la ejecución del cobro coactivo de las garantías del crédito. Este proceso puede resultar en una renegociación con el cliente, lo cual se traduce en un crédito reestructurado.

d. Operaciones

El proceso de operaciones agrupa todas las actividades necesarias, para que los clientes puedan realizar cualquiera de las siguientes transacciones: depósitos, retiros, transferencias, pago de servicios y pago de obligaciones. Por otro lado, comprende las tareas relacionadas al cierre de caja diario y el balance de operaciones.

e. Captaciones

Este proceso gestiona el incremento de la cartera de clientes y por ende la participación en el mercado de la microfinanciera. La forma de obtención de nuevos clientes, la distribución de información adecuada y detallada a personas que sean identificadas como potenciales clientes para la microfinanciera.

f. Riesgo Crediticio

Es el proceso encargado de analizar los diferentes tipos de crédito que se han otorgado, asignar la provisión necesaria para estos créditos y planificar y ejecutar acciones, para aminorar el riesgo de que un cliente no cumpla con sus obligaciones.

g. Riesgo Operativo

Es el proceso encargado de gestionar, todos los eventos que involucran una pérdida por operaciones, ya sea por deficiencias o fallas en los procesos internos, fallas del personal, de la tecnología de la información o por una ocurrencia de un evento externo. Su finalidad es disminuir la probabilidad de ocurrencia de estos eventos y aminorar su impacto.

h. Riesgo de Mercado

Este proceso administra, todos los eventos que involucran la probabilidad de pérdidas financieras, en posiciones dentro y fuera del balance, derivadas de las fluctuaciones de los precios de mercado, como las tasas de interés, los tipos de cambio y los precios de acciones.

Considerando lo propuesto por Berrospi Liu y Valencia Zuñiga (2013), se muestran en el siguiente mapa los macro procesos que se presentan, dentro de las microfinancieras, los cuales están clasificados por niveles: estratégicos, operativos y de apoyo.

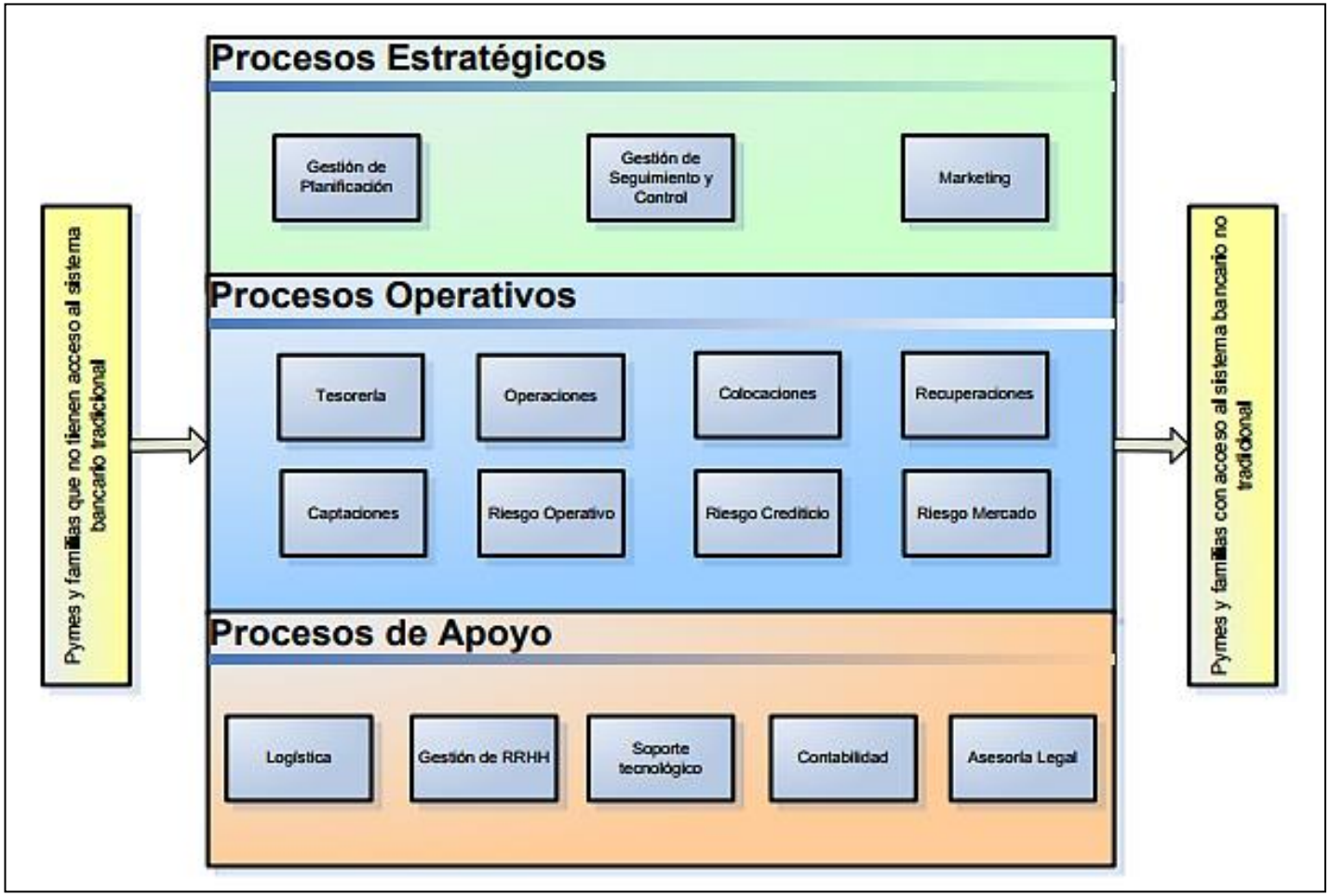


Figura 8. Mapa de macroprocesos de una microfinanciera

Fuente: (Berrospi Liu y Valencia Zuñiga 2013)

CAPÍTULO II MATERIALES Y MÉTODOS

1.1 Diseño de la investigación

El tipo de estudio es cuantitativo, transversal no experimental descriptivo.

El diseño de contrastación de hipótesis, es del tipo cuasi experimental porque la muestra no ha sido tomada probabilísticamente, sino que es en base a la accesibilidad a las microfinancieras de la región Lambayeque. Se usará un modelo de preprueba/postprueba con un solo grupo:

G O1 X O2

Dónde:

- ✓ G: Caso de estudio seleccionado.
- ✓ O1: Contribuir a la continuidad del negocio en las microfinancieras de la región Lambayeque, antes de la aplicación el modelo de gestión de riesgos.
- ✓ X: Modelo de gestión de riesgos de TI.
- ✓ O2: Contribuir a la continuidad del negocio en las microfinancieras de la región Lambayeque, después de la aplicación el modelo de gestión de riesgos.

1.2 Población y Muestra

Para el diagnóstico inicial de esta investigación, se consideró a las microfinancieras que operan en la región Lambayeque reconocidas por la SBS, que son un total de 14 empresas según lo define la Asociación de Microfinancieras del Perú (ASOMIF):

- Caja Metropolitana
- Caja Arequipa
- Caja Trujillo
- Caja Piura
- Caja Rural Sipán
- Mi Banco
- Edpyme Acceso Crediticio
- Edpyme Alternativa
- Edpyme Inversiones La Cruz
- Edpyme Solidaridad y Desarrollo Empresarial
- Compartamos Financiera
- Financiera Confianza
- Financiera Efectiva
- Financiera TFC

De éstas, solo se consideró como muestra a aquellas que tienen su sede central en la región Lambayeque, que en total son 3 empresas cuyas características se detallan a continuación:

- **Microfinanciera 1**

  Inició sus operaciones en 1995. La actividad crediticia y de negocios en general se desarrolla a través de sus oficinas ubicadas en la ciudad de Chiclayo, Lambayeque–Perú. Cuenta con 6 agencias y 3 oficinas informativas para la atención de clientes, dos ubicadas en la ciudad de Chiclayo, una en la ciudad de Jaén del departamento de Cajamarca, una en la ciudad de Chepén una en la ciudad de Trujillo del departamento de La Libertad y otra en Nueva Cajamarca departamento de San Martín.

- **Microfinanciera 2**

  Es una institución de microfinanzas, con sede principal en la ciudad de Chiclayo, Lambayeque – Perú, 20 agencias y 7 oficinas informativas distribuidas en la región nororiente del país. Sus orígenes se remontan al año 1992, cuando la Cámara de Comercio y Producción de Lambayeque suscribió un convenio con el Banco Interamericano de Desarrollo para impulsar el crecimiento de la pequeña y micro empresa, el mismo que se inicia otorgando préstamos y finaliza exitosamente el año 2001. Luego de este proceso, en setiembre del 2001 empieza a operar en el mercado como una entidad financiera regulada por la SBS.

- **Microfinanciera 3**

  Es una entidad que forma parte de un grupo económico de empresas retail, supervisada por la SBS y especializada en el otorgamiento de créditos al sector emergente.

  Inició sus operaciones en el año 1999 como una entidad de desarrollo para la pequeña y microempresa (EDPYME) convirtiéndose en el 2010 en entidad financiera.

  A través de más de 193 oficinas a nivel nacional, otorga el financiamiento a los clientes que adquieren productos en las empresas vinculadas al grupo. Habiendo obtenido en los últimos 6 años ratios de cartera, solidez y rentabilidad por encima del promedio del sector.

En el Anexo 1, se muestra un cuadro más detallado de la comparación de estas entidades microfinancieras.

1.3 Métodos y Técnicas de Recolección de Datos

Los métodos de recolección de datos que se emplearon en esta investigación son:

a) Observación Activa

Las investigadoras observaron in-situ el desarrollo de las principales operaciones lo que permitió conocer más de cerca la realidad de las microfinancieras. Se puso especial atención en los procesos críticos, para determinar los riesgos que causen su interrupción.

b) Estudio de Casos

Se estudió la situación particular de 3 de las microfinancieras de la región Lambayeque, en relación con la gestión de riesgos de TI.

En esta investigación se emplearon las siguientes técnicas de recolección de datos:

a) Encuesta

Se aplicó una encuesta, con el fin de conocer las prácticas de gestión de riesgos según las fases que propone la ISO/IEC 31000. La encuesta estará dirigida a:

- Gerencia de TI.
- Gerencia de riesgos.
- Oficialía de seguridad de TI.
- Auditor interno.

b) Revisión de Documentación

Se realizó la revisión de documentos estratégicos, administrativos, legales y técnicos relacionados a la gestión de riesgos que permitan conocer las prácticas de gestión de riesgos que tienen implementadas y sus necesidades para el cumplimiento de exigencias normativas. Los documentos que se revisaron fueron:

- Plan estratégico de TI.
- Política de gestión de seguridad de la información.
- Manual de gestión de riesgos operativos de TI.
- Informe anual de observaciones de la SBS.

- Normativas SBS relacionadas a la gestión de riesgos, seguridad de la información y continuidad del negocio.
- Manuales técnicos.

1.4 Técnicas de Procesamiento de Datos

Se aplicó una encuesta a los directores y gestores de riesgos, en 3 microfinancieras de la región Lambayeque, para obtener un diagnóstico de cómo se gestionan los riesgos de tecnologías de información (TI) y a partir de ello determinar un perfil de este tipo de empresas. Para esto, se usó el análisis e interpretación de datos usando gráficos del programa Microsoft Excel.

Además se revisó la documentación sobre políticas, planes, manuales e informes relacionados a la gestión de riesgos de TI.

En base a la información recolectada y luego de realizar el análisis correspondiente, se procedió con el diseño del modelo de gestión de riesgos de TI y para evaluar su validez se usó la herramienta estadística SPSS (Paquete Estadístico para las Ciencias Sociales). Finalmente, se aplicó el modelo propuesto a un caso de estudio para probar su aplicabilidad en un entorno real.

CAPÍTULO III RESULTADOS Y DISCUSIÓN

1.1 Análisis de la situación actual de las microfinancieras relacionado a la gestión de riesgo de TI

Se aplicó una encuesta a los directores y gestores de riesgos de 3 microfinancieras de la región Lambayeque, para obtener un diagnóstico de cómo se gestionan los riesgos de tecnologías de información (TI) y a partir de ello determinar un perfil de este tipo de empresas. Además se revisó documentación sobre políticas, planes, manuales e informes relacionados a la gestión de riesgos de TI, de las cuales hacen uso cada una de estas organizaciones.

Esta encuesta permitió reconocer el cumplimiento de las pautas que propone la norma ISO/IEC 31000. En el Anexo 2, se puede mostrar el cuestionario que fue dirigido a los principales gestores de riesgos de las 3 entidades microfinancieras.

En la encuesta se ha evaluado cada una de las fases establecidas en la ISO/IEC 31000 para la gestión de riesgos, además se ha incluido el análisis de impacto (BIA) para evaluar la continuidad del negocio. De esta manera, se ha podido conocer, el nivel de cumplimiento de la gestión de riesgos de TI, en el sector microfinanciero de la región Lambayeque, con las normas internacionales según como se muestra en el siguiente gráfico:

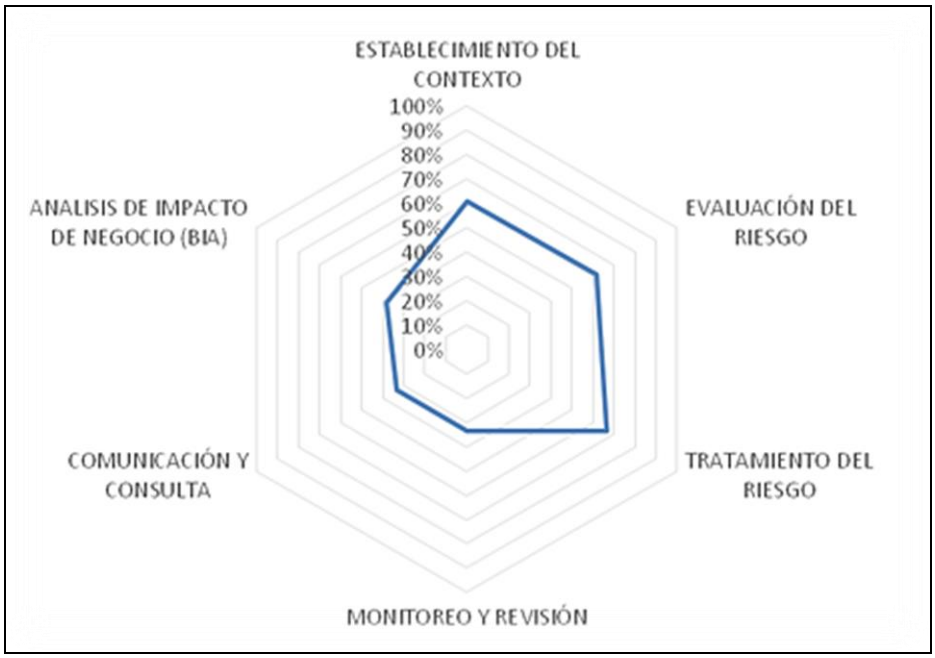


Figura 9. Diagnóstico la gestión de riesgos de TI en las entidades microfinancieras

A continuación se detalla el análisis del diagnóstico del sector microfinanciero con respecto a cada fase propuesta por la ISO/IEC 31000:

Con respecto al **establecimiento del contexto**, se puede observar que en las entidades microfinancieras, si se cuenta con un marco de referencia para la gestión de riesgo de TI, según la exigencia de las normativas de la SBS, pero un 33.33% manifestaron que los objetivos, el alcance y las actividades no están bien definidos. La gestión de riesgos está de acuerdo a los objetivos de la organización en cuanto al contexto interno y externo, pero no se cuentan con los recursos necesarios y no se tienen claros los criterios, para evaluar la importancia de los riesgos. Además, las entidades microfinancieras, cuentan con manuales para gestionar sus riesgos de TI, que es una guía para la gestión de los riesgos de acuerdo con lo interpuesto en el reglamento para la gestión del riesgo operacional (Resolución S.B.S. N° 2116-2009), gestión de la continuidad del negocio (Circular G-139-2009) y gestión de la seguridad de la información (Circular G-140-2009).

Relacionado a la **evaluación del riesgo**, se pudo observar que los activos están identificados y registrados como parte del catálogo de activos de la

organización, pero solo un 66.66%, afirmó que tiene claramente identificados tanto las vulnerabilidades como las amenazas, a los que están expuestos, sólo un 33.33% identifica cuáles son las fuentes del riesgo, así como las áreas y procesos que son impactados. En la identificación de los riesgos se involucra al personal experto en el tema, pero el resto del personal no tiene información pertinente y actualizada para identificar los riesgos de TI. Sin embargo, los riesgos son priorizados en función de su impacto en el logro los objetivos organizacionales. También, se percibe un completo interés en contar con procedimientos o métodos que les permitan asegurar los activos fundamentales para la operatividad de las instituciones.

Respecto al **tratamiento del riesgo**, las entidades microfinancieras, cuentan con un proceso de tratamiento de riesgos, pero éstos no están integrados a los procesos de gestión de la organización y no se realiza un monitoreo periódico de la gestión de riesgos, por lo que no se determina su magnitud para implantar los controles necesarios para minimizarlos. Un 66.66% manifiesta que las estrategias de tratamientos de riesgos se ejecutan teniendo en cuenta el orden de prioridad, según la evaluación de riesgos y los gestores de riesgos normalmente reconocen el riesgo residual, luego de ser aplicados los controles.

En lo que respecta al **monitoreo y revisión,** las entidades microfinancieras, cuentan con un proceso formal de monitoreo de riesgos, pero éste no se realiza de manera periódica, ni se tienen claramente identificadas las tareas y responsabilidades de cada gestor de riesgos.
Relacionado a la **comunicación y consulta**, el 33% de los encuestados, no ha desarrollado planes de comunicación de riesgos, lo que dificulta la toma de decisiones de los altos directivos, sin embargo un 66% manifiesta que si se toman en cuenta las opiniones de los involucrados para gestionar los riesgos de TI.

Respecto al **análisis del impacto del impacto de negocio,** se puede notar que las instituciones cuentan con una política de continuidad de negocio y que está disponible para ser accedida por los trabajadores, pero la

cultura organizacional de las instituciones no está alineada a dichas políticas dado que los empleados no acceden a esa información. Las organizaciones no son conscientes de la importancia de la política de continuidad del negocio, dado que se percibe que las políticas solo son acatadas por motivos de supervisión de la SBS, las cuales son realizadas en ciertos periodos del año mediante auditorias y que sólo se concentran en corregir observaciones como resultado a dichas auditorías.

Por último, se percibe que no existe un proceso formal y documentado para la comprensión de la organización a través de un BIA.

1.2 Análisis de estándares y metodologías relacionados con la gestión de riesgos

Para realizar la propuesta del método de gestión de riesgos de TI aplicado al sector microfinanciero, se han evaluado los siguientes estándares, marcos de trabajo y metodologías:

- ISO/IEC 31000:2009
- ISO/IEC 27005:2008
- ISO/IEC 22301:2012
- OCTAVE
- MAGERIT
- COBIT 5 para Riesgos

A continuación se muestra el desarrollo del análisis, como resultado de esto se obtiene la metodología propuesta en el punto 1.3.

a. Establecimiento del contexto

En esta fase se toma como base la norma ISO/IEC 31000 donde se establece que se deben definir de los parámetros internos y externos que deben tenerse en cuenta en la gestión de riesgos.

Definir el contexto externo

En la siguiente tabla se muestra una comparación de los puntos que deben incluir el análisis del contexto interno según las normas.

Tabla 1. Contexto externo según ISO/IEC 31000 y COBIT 5

ISO 31000	COBIT 5
- La cultural, social, político, jurídico, reglamentario, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local. - Factores clave y las tendencias con repercusiones en los objetivos de la organización. - Las relaciones con las partes involucradas, internas y externas, y sus percepciones y valores.	- Factores económicos y de mercado. - Tasa de cambio del mercado/ciclo de vida del producto - Industria y competencia. - Situación geopolítica. - Ambiente regulatorio. - Estado de la tecnología y su evolución. - Panorama de amenazas.

En el caso de las instituciones microfinancieras, se considera que se debe analizar los siguientes criterios:

- **Sociocultural:** para conocer cómo se van desarrollando la población objetivo de las microfinancieras orientado principalmente a sectores bajos.

- **Económico:** los cambios económicos, forzarían a adoptar nuevas estrategias de captación de clientes.

- **Competitivo:** dado que existen en el mercado microfinancieras orientadas a sectores bajos de la población.

- **Tecnológico:** porque facilita brindar servicios financieros de forma más eficaz y menos costosa.

- **Reglamentario:** el sector microfinanciero está fuertemente regulado por la superintendencia de banca y seguros.

- **Proveedores:** las microfinancieras tercerizan, principalmente los servicios relacionados con telecomunicaciones, que resultan básicos para las principales operaciones.

Definir el contexto interno

La norma establece que el contexto interno puede incluir:

Tabla 2. Contexto interno según ISO/IEC 31000 y COBIT 5

ISO 31000	COBIT 5
- Gobernanza, la estructura organizativa, las funciones y responsabilidades. - Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos. - La capacidad, entendida en términos de recursos y conocimientos (capital, por ejemplo, tiempo, Personas, procesos, sistemas y tecnologías). - La cultura de la organización. - Los sistemas de información, flujos de información y la toma de decisiones (tanto formales como informales). - Relaciones con, y las percepciones y los valores de, grupos de interés internos. - Normas, directrices y modelos adoptados por la organización. - Forma y extensión de las relaciones contracturales.	- Metas y objetivos de la empresa. - Importancia estratégica de TI para la empresa. - Complejidad de TI. - Complejidad de la empresa y grado de cambio. - Modelo operativo. - Prioridades estratégicas. - Cultura de la empresa. - Capacidad financiera.

En el caso de las instituciones microfinancieras, se considera que se debe analizar los siguientes criterios:

- **Estructura organizacional:** para comprender cómo están organizados los roles y las jerarquías para la toma de las decisiones.

- **Objetivos organizacionales:** es importante conocer las metas globales que tienen planteada la organización.

- **Cultura organizacional:** en el sector financiero se tiene la cultura orientada a dar buen servicio al cliente.

- **Sistemas de información:** porque dan soporte a las principales operaciones de las microfinancieras.

b. Análisis de impacto de negocio

La cláusula 8.2.2 del estándar internacional en continuidad del negocio ISO/IEC 22301:2012, menciona que uno de los requisitos, es realizar un análisis de impacto de negocio con la finalidad de definir el orden y los tiempos de recuperación de las actividades críticas, que soportan los servicios claves (RTO – Tiempo Objetivo de Recuperación) y el establecer esquemas de tiempo priorizados para reanudar operaciones (MTPD - Periodo máximo tolerable de interrupción).

El estándar ISO/IEC 22301:2012 en la cláusula 8.2.3 habla de la evaluación de riesgos que pudieran alterar las actividades priorizadas, es por eso que esta fase retroalimentará a la fase 3 de identificación de riesgos.

- **Identificación de procesos:** Como punto inicial se ha creído conveniente partir con la identificación de los procesos del negocio para luego identificar los procesos críticos.

- **Evaluación del impacto del negocio:** Consiste en medir el impacto de los procesos, teniendo en cuenta los aspectos financieros, regulatorios y reputaciones.

- **Establecimiento de periodos de tiempo:** Permite medir los tiempos de recuperación y la tolerancia máxima de interrupción de los procesos.

- **Establecimiento de nivel de criticidad de los procesos:** En base a la evolución de impacto y el establecimiento de periodos de tiempo se analiza cada proceso y se identifican los procesos críticos de la organización que dependen del soporte del área de TI.

- **Identificación de dependencias y recursos críticos:** Identificado los procesos críticos, se identifican también los recursos y activos que dan soporte a estos procesos.

- **Establecimiento de estrategias:** Luego de haber identificado los activos y los riesgos a los cuales están expuestos, se pueden establecer estrategias, de tal manera que se consiga la continuidad del negocio.

c. Identificación del riesgo

Para identificar los riesgos, primero se procederá con la identificación y valoración de los activos, según cómo se propone en MAGERIT. Luego, a partir de estos activos se identificarán vulnerabilidades y amenazas a los que está expuesto para lo cual se han definido los siguientes procesos:

Identificar activos

MAGERIT propone que para cada activo hay que determinar una serie de características que lo definen:

- Código, típicamente procedente del inventario.
- Nombre (corto).

- Descripción (larga).
- Tipo (o tipos) que caracterizan el activo.
- Unidad responsable.
- Persona responsable.
- Ubicación, técnica o geográfica.
- Cantidad.
- Otras características específicas del tipo de activo.

De estas características, se considera que para el sector microfinanciero, resulta información suficiente, registrar al activo con los siguientes identificadores:

- Código.
- Nombre.
- Descripción.
- Responsable.
- Tipo.

Para la clasificación de los activos algunas normas y estándares proponen lo siguiente.

Tabla 3. Clasificación de Activos de Información

MAGERIT	ISO 27005:2008	OCTAVE
Esenciales - Información - Servicios **Arquitectura del Sistema** - Datos / Información - Claves Criptográficas - Servicios - Software – Aplicaciones informáticas - Hardware - Equipamiento	**Primarios** - Actividades y Procesos del negocio - Información **De soporte** - Hardware - Software - Redes - Personal - Ambientes físicos - Estructura Organizacional	- Sistemas - Información - Aplicaciones - Personas

MAGERIT	ISO 27005:2008	OCTAVE
informático - Soporte de Información - Equipamiento Auxiliar - Personal		

En base a esto, se establece la clasificación más adecuada en el contexto microfinanciero:

- **Procesos del negocio:** identificar los procesos más importantes que para las microfinancieras están relacionados con la colocación y captación de créditos.

- **Servicios:** detallar los principales procesos de TI que dan soporte a las operaciones de las microfinancieras.

- **Software:** reconocer los principales programas informáticos que funcionan en producción.

- **Hardware:** identificar los equipos informáticos involucrados en los procesos core de las microfinancieras.

- **Soporte de información:** los medios de almacenamiento de la información.

Valorar activos

La norma (ISO/IEC 27005:2008), recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar, el riesgo en la seguridad de la información de la organización, teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información del negocio.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.

- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

Analizando las principales metodologías, éstas proponen distintos aspectos para valorar los activos que se resumen en la siguiente tabla:

Tabla 4. Aspectos para la valoración de activos

MAGERIT	COBIT	OCTAVE
Dimensiones - Disponibilidad. - Integridad de los datos. - Confidencialidad de los datos. - Autenticidad de los usuarios del servicio. - Autenticidad del origen de los datos. - Trazabilidad del servicio. - Trazabilidad de los datos.	**Criterios** - Efectividad. - Eficiencia. - Confidencialidad. - Integridad. - Disponibilidad. - Cumplimiento. - Confiabilidad.	**Categorías** - Disponibilidad. - Integridad de los datos. - Confidencialidad de los datos.

Para el contexto microfinanciero, se considera lo indicado por OCTAVE que se ajusta a lo exigido por la SBS en la circular G-140-2009 de riesgos de tecnología de información:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Cumplimiento Normativo.

Para valorar cada criterio se establece una escala estandarizada usando la escala de Likert del 1 a 5.

Identificar amenazas y vulnerabilidades

La norma ISO/IEC 27005:2005 propone un catálogo de amenazas asociado a las vulnerabilidades de cada tipo de activo. A partir de la identificación de amenazas, se obtiene la lista de riesgos asociados a cada activo.

Según MAGERIT, el objetivo de esta tarea es caracterizar el entorno al que se enfrenta el sistema, ¿qué puede pasar?, ¿qué consecuencias se derivarían? y ¿cuál es la probabilidad que pase?. Para cada amenaza de cada activo, conviene registrar la siguiente información:

- Estimación de la frecuencia de la amenaza.
- Estimación del daño (degradación) que causaría su materialización.
- Explicación de las estimaciones de frecuencia y degradación.

En base a esto se propone identificar las amenazas según a las vulnerabilidades que explotan relacionado a un activo.

d. Análisis del riesgo

El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, consecuencias y la probabilidad de materialicen. (ISO/IEC 31000:2009).

Definir los criterios del riesgo

El riesgo, es analizado mediante la determinación de la probabilidad de ocurrencia y el impacto que genere (ISO/IEC 31000:2009). Para cada uno de estos factores, se debe establecer una escala de valorización. Además, en función del producto de la probabilidad e impacto se define un nivel de riesgo (alto, medio, alto, extremo).

La norma ISO/IEC 27005, utiliza dos enfoques para emitir una valoración: elementos cualitativos o cuantitativos (o bien, una

combinación de ambos), que permitan determinar la severidad de los riesgos identificados y analizados previamente:

- **Estimación cuantitativa:** asigna valores monetarios a riesgos específicos, por lo que tiene como punto de partida la determinación de una pérdida potencial asociada a la materialización de una o más amenaza.

- **Estimación cualitativa:** valoración realizada a través de las características que tienen como base un escenario de amenaza sobre los activos, y generalmente está asociado a una calificación de los riesgos que utiliza como parámetros cualidades como alto, medio o bajo.

Para el caso de las entidades microfinancieras se considera la valoración cualitativa en función de la continuidad del negocio valorando que tanto afecta la materialización de un riesgo en la continuidad de las operaciones críticas.
La norma ISO/IEC 27005 también propone la elaboración de un mapa de riesgos que estima el nivel de riesgo en función de la probabilidad e impacto.

Estimar el riesgo

Establecidos los criterios del riesgo, se procede a valorar el impacto de la probabilidad, si llega a materializarse una amenaza, de esta manera se identifican los riesgos y su nivel de criticidad. Es decir, por cada riesgo se examina el impacto y probabilidad y partir de ello se obtiene el nivel de riesgo.

e. Evaluación del riesgo

El propósito de la evaluación de riesgos es ayudar en la toma de decisiones, basada en los resultados de análisis de riesgos, sobre riesgos que necesitan tratamiento y la prioridad para la aplicación del tratamiento. Además supone la comparación del nivel de riesgo

identificado durante el proceso de análisis con criterios de riesgo (ISO/IEC 31000:2009).

Priorizar riesgos

El estándar ISO/IEC 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada.

En esta propuesta, se opta por la realización de una matriz de calor, la cual tiene como criterios la probabilidad que cierta amenaza explote cierta vulnerabilidad y el impacto al negocio estimado que la ocurrencia del riesgo pueda ocasionar al negocio.

Valorar riesgos

Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables. (ISO/IEC Guía 73:2002)

f. Tratamiento del riesgo

El tratamiento del riesgo, consiste en seleccionar una o más opciones de modificación de los riesgos, y la aplicación de esas opciones. Una vez en marcha, los tratamientos de proporcionar o modificar los controles existentes. (ISO/IEC 31000:2009).

Seleccionar estrategias de tratamiento

En relación al tratamiento de riesgos, se proponen distintas opciones de respuestas:

Tabla 5. Opciones de tratamiento de riesgos según estándares

FUENTE	OPCIONES DE TRATAMIENTO				
COBIT 5	Evitar	Transferir Compartir	Mitigar	Aceptar	--
ISO 27005	Evitar	Transferir	Reducir	Retener	--

FUENTE	OPCIONES DE TRATAMIENTO				
ISO 31000	Evitar Remover la fuente del riesgo	Transferir	Cambiar la naturaleza y magnitud de posibilidad Cambiar las consecuencias	Retener por decisión.	Buscar una oportunidad
MAGERIT	Eliminación	Compartición	Mitigación	Financiación	

Para el modelo se considera lo propuesto en el estándar ISO/IEC 27005:2005.

Proponer planes de acción

La norma ISO/IEC 22301 plantea la elaboración de planes de acción: correctivos o preventivos, para llevar a cabo las estrategias de tratamiento de riesgos y plantea.

g. Monitoreo y revisión

La norma ISO/IEC 31000 lo define como un control continuo, supervisar, observar críticamente o determinar el estado a fin de determinar el cambio del nivel de rendimiento requerido o esperado.

Como en la fase anterior se definieron planes de acción para el tratamiento de los riesgos, en esta etapa se deben revisar y controlar el resultado de la ejecución de dichos planes de acción.

h. Comunicación y consulta

La norma ISO/IEC 31000, define procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir y obtener información y para entablar un diálogo con las partes interesadas en relación con la gestión del riesgo.

1.3 Desarrollo de la Propuesta

Dentro del análisis de las metodologías y estándares relacionados con la gestión de riesgos de tecnologías de información y cumpliendo los criterios

mínimos para la identificación y tratamiento de los riesgos asociados a las tecnologías de la información (TI) establecidos por la SBS en el reglamento para la gestión del riesgo operacional (Resolución S.B.S. N° 2116-2009), la gestión de la continuidad del negocio (Circular G-139-2009) y la gestión de la seguridad de la información (Circular G-140-2009). A partir de esto, se han identificado las fases que mejor se adaptan a las necesidades del contexto de las entidades microfinancieras de la región Lambayeque.

Como estándar base, se partió de las fases propuestas en la norma internacional ISO/IEC 31000:2009, según como se explica en el punto 2.2.3.3 del capítulo anterior y en cada fase se han incorporado las metodologías y estándares explicados en el punto 2.2.3.2 del mismo capítulo. Adicionalmente, se incluyó el análisis de impacto de negocio (BIA) propuesto por la norma ISO/IEC 22301 para alinear el análisis de riesgos con la continuidad del negocio.

En la siguiente figura se esquematizan las fases que se han contemplado en el método propuesto.

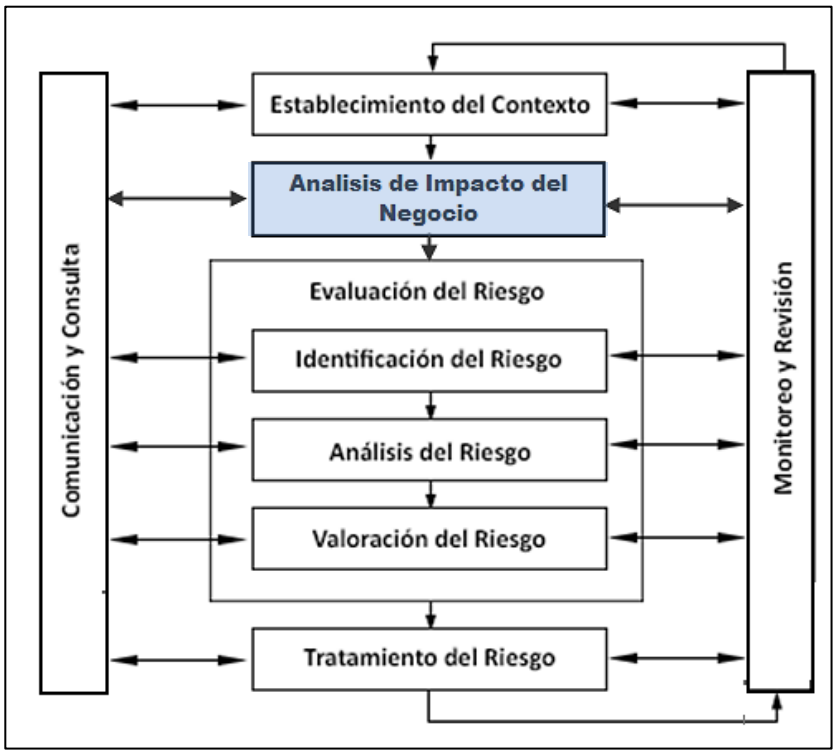


Figura 10. Metodología propuesta para la gestión de riesgos de TI
Fuente: Adaptado de la norma ISO/IEC 31000

Fase I: Establecimiento del contexto

Un verdadero pilar de la norma, es establecer el contexto en el que opera la organización que consiste en la definición del alcance y los parámetros internos y externos que deben tenerse en cuenta en la gestión de riesgos de TI.

Esta fase comprende dos actividades:

Actividad 1: Definir el contexto externo

El contexto externo, es el entorno ajeno a la organización en el ésta busca alcanzar sus objetivos. Comprender el contexto externo, es importante para tener conocimiento del panorama global alrededor de las microfinancieras, que permite aprovechar las oportunidades y evitar las amenazas. En la siguiente tabla se propone una plantilla para la descripción del contexto externo.

Tabla 6. Plantilla para descripción del ambiente externo

DEFINICIÓN DE CONTEXTO EXTERNO		**CÓDIGO: P001**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Sociocultural	Se incluyen principalmente aspectos demográficos y culturales relacionados al sector objetivo de la microfinanciera que influye directamente en las estrategias de la empresa. Fuente de información: Instituto Nacional de Estadística e Informática (INEI).
2	Económico	Se consideran los cambios económicos que pueden generar oportunidades o amenazas en el desarrollo de las actividades de la microfinanciera. Fuente de información: Banco Central de Reserva del Perú (BCP).
3	Competitivo	Conformado por las microfinancieras que operan en la región Lambayeque. Fuente de información: Asociación de Instituciones de Microfinanzas del Perú (ASOMIF).

DEFINICIÓN DE CONTEXTO EXTERNO		CÓDIGO: P001
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
N°	**ASPECTO**	**DESCRIPCIÓN**
4	Tecnológico	Abarca los cambios tecnológicos que influencian en las estrategias de las microfinancieras que abarcan temas como: FinTech, cloud computing, dinero electrónico, omnicanalidad, internet de las cosas, ciberseguridad. Fuente de información: INEI, revistas de tecnología.
5	Reglamentario	Relacionado con las normas que controlan y legislan en el sector microfinanciero. Fuente de información: SBS, INDECOPI, BCR, SUNAFIL, SUNAT.
6	Proveedores	Conformado por empresas que brindan servicios como tercero para dan soporte a los procesos de las microfinancieras. Fuente de información: Lista de proveedores de servicios.

Actividad 2: Definir el contexto interno

El contexto interno, está conformado por los elementos dentro de la organización, que pueden influir en la manera en la que se va a gestionar el riesgo. El proceso de gestión de riesgos debe estar alineado con la cultura de la organización, procesos, estructura y estrategia. En la siguiente tabla se propone una plantilla para la descripción del contexto interno.

Tabla 7. Plantilla para descripción del ambiente externo

DEFINICIÓN DE CONTEXTO INTERNO		CÓDIGO: P002
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Estructura organizacional	Se refiere a la disposición de roles que se agrupan para formar áreas o departamentos, estableciendo responsabilidad y autoridad.

DEFINICIÓN DE CONTEXTO INTERNO		CÓDIGO: P002
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
N°	**ASPECTO**	**DESCRIPCIÓN**
		Fuente de información: Organigrama empresarial, Manual de Organización y funciones.
2	Cultura organizacional	Conformado por las actitudes, experiencias, creencias y valores característicos de la institución. Fuente de información: Plan estratégico empresarial, misión, visión, valores.
3	Objetivos organizacionales	Metas a las cuales está orientada la organización alineadas a la misión y visión. Fuente de información: Plan estratégico empresarial.
4	Sistemas de información	Conformado por el software que maneja la organización que permite para optimizar procesos, tiempos, recursos humanos; agilizando los procesos. Fuente de información: Inventario de software.

Fase II: Análisis de impacto de negocio

Este análisis permite determinar el impacto en el tiempo que ocasionaría una interrupción de los principales procesos de la Financiera.

Actividad 1: Identificar procesos

Esta etapa se identifica los procesos críticos de la organización.

A través de un mapa de procesos se pueden identificar los procesos de la microfinanciera y por cada uno se debe elaborar un diagrama identificando sus principales actividades y actores. En la tabla se propone una plantilla con un mapa de procesos genérico para microfinancieras.

Tabla 8. Plantilla de identificación de procesos

IDENTIFICACIÓN DE PROCESOS	CÓDIGO: P003
Elaborado por: _____ Revisado por: _____ Aprobado por: _____	

Actividad 2: Evaluar el impacto del negocio

Se evalúa el impacto de los procesos en el negocio para lo cual se ha considerado los aspectos financieros, regulatorios y reputacionales, las cuales se muestran a continuación según las escalas de Liker.

- **Impacto Financiero**

  Pérdidas monetarias que la compañía tendría que afrontar al dejar de ejecutarse el proceso, tiene afectación directa en las utilidades de la empresa.

Tabla 9. Criterios para evaluar el impacto financiero

FINANCIERO (F)	VALOR
Afecta de manera insignificante a la continuidad de la empresa.	1
Afecta poco a la continuidad de la empresa.	2
Afectación regular a la continuidad de la empresa.	3
Afectación grande y compromete en mayor parte de la continuidad de la empresa.	4
Afecta toda la continuidad del negocio	5

La microfinanciera debe definir qué significa poco, regular y grave de acuerdo a su realidad.

- **Impacto Regulatorio**

  Son las consecuencias (amonestaciones, penalizaciones o multas), de tipo legal o fiscal que la compañía, pueda tener en el caso de no cumplir con lo establecido en normativas internas o externas.

Tabla 10. Criterios para evaluar el impacto regulatorio

REGULATORIO (R)	VALOR
Amonestación por incumplimiento de normativas o contratos con clientes.	1
Produce una falta leve en el cumplimiento de normativas o contratos con clientes.	2
Produce una falta grave en el cumplimiento de algún contrato con clientes que obliga a renegociar.	3
Produce una falta grave en el cumplimiento de normativas o contratos con clientes que acarrea responsabilidades legales.	4
Deja a la organización al margen de la ley.	5

La microfinanciera debe definir qué significa una falta grave y una falta leve de acuerdo a su realidad.

- **Impacto Reputacional**

  Son las consecuencias negativas que la compañía tendría que afrontar debido a una mala gestión dañando así su reputación.

Tabla 11. Criterios para evaluar el impacto reputacional

REPUTACIONAL (RE)	VALOR
Conocido solo por los trabajadores de la Financiera.	1
Conocido solo por clientes, no está en los medios de comunicación.	2
Conocido por medios locales, generando comentarios adversos.	3
Conocido por medios nacionales, generando comentarios adversos.	4
Daños a la imagen de la marca y campaña continuada en medios nacionales.	5

Luego en base a los procesos identificados en la etapa anterior se debe completar la siguiente plantilla:

Tabla 12. Plantilla de procesos que impactan en el negocio

IMPACTO EN EL NEGOCIO DE LOS PROCESOS						CÓDIGO: P004
Elaborado por: _____ Revisado por: _____ Aprobado por: _____						
UNIDAD DE NECOGIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**IMPACTO**		
				F	**R**	**RE**
Área dueña del proceso	Nombre del macro proceso	Nombre del proceso	Servicio de TI que soporta al proceso	Ver Tabla 9	Ver Tabla 10	Ver Tabla 11

Actividad 3: Establecer periodos de tiempo

Después de haber establecido el impacto de cada proceso, se establecen los parámetros para valorar el tiempo objetivo de recuperación (RTO), el punto objetivo de recuperación (RPO) y el periodo máximo tolerable de interrupción (MTPD).

- **Punto Objetivo de Recuperación (RPO)**

  Es la pérdida de datos máxima tolerable, que se acepta ante una situación de desastre. Según las indagaciones con el operador de una de las financieras estudiadas, se identificó que la frecuencia de backup (RPO) se realiza al finalizar cada día (24 horas). Si no hay pérdida de datos aceptable, el RPO es cero.

- **Tiempo Objetivo de Recuperación (RTO)**

  Es el tiempo establecido por la empresa, para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción. Según el proceso a evaluar se detalla el periodo máximo de interrupción que podría soportar cada proceso identificado en la organización.

Tabla 13. Criterios para estimar el RTO

RTO	VALOR
La actividad o el proceso requieren alta disponibilidad (100%).	1
La actividad o el proceso no pueden estar interrumpidos más de 4 horas.	2
La actividad o el proceso no pueden estar interrumpidos más de 8 horas.	3
La actividad o el proceso no pueden estar interrumpidos más de 24 horas.	4

Los tiempos establecidos se obtuvieron a partir del análisis de 3 microfinancieras de la región Lambayeque.

- **Periodo Máximo Tolerable de Interrupción (MTPD)**

  Es el periodo de tiempo, luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado.

Tabla 14. Criterios para estimar el MTPD

MTPD	VALOR
La viabilidad de la empresa es afecta seriamente en la primera hora luego de la interrupción.	1
La viabilidad de la empresa es afecta seriamente después de 8 horas luego de la interrupción.	2
La viabilidad de la empresa es afecta seriamente después de 24 horas luego de la interrupción.	3
La viabilidad de la empresa es afecta seriamente después de 72 horas luego de la interrupción.	4

Los tiempos establecidos se obtuvieron a partir del análisis de 3 microfinancieras.

Según los parámetros establecidos, se debe completar la siguiente plantilla:

Tabla 15. Plantilla de tiempos por procesos

ESTABLECIMIENTO DE TIEMPOS POR PROCESOS						CÓDIGO: P005
Elaborado por: _____ Revisado por: _____ Aprobado por: _____						
UNIDAD DE NECOGIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**RTO**	**RPO**	**MTPD**
Área dueña del proceso	Nombre del macro proceso	Nombre del proceso	Servicio de TI que soporta al proceso	Ver Tabla 13	Tiempo en horas	Ver Tabla 14

Actividad 4: Establecer el nivel de criticidad de los procesos

El nivel de criticidad de los procesos se estima según lo establecido en las escalas del Máximo Tiempo Tolerable de Interrupción (MTPD):

Tabla 16. Matriz de Impacto vs. Tiempo

ESCALA	MTPD
No Crítico	De 7 días a más
Sensible	De 4 a 7 días
Vital	De 13 horas a 3 días
Crítico	De 0 a 12 horas

Los tiempos establecidos se obtuvieron a partir del análisis de 3 microfinancieras.

Como resultado de esta fase se debe completar el siguiente formato:

Tabla 17. Plantilla de procesos según su criticidad

CRITICIDAD DE LOS PROCESOS					**CÓDIGO: P006**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____					
UNIDAD DE NEGOCIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**MTPD**	**ESCALA**
Área dueña del proceso	Nombre del macro proceso	Nombre del proceso	Servicio de TI que soporta al proceso	Ver Tabla 14	Ver Tabla 16

Fase III: Identificación del riesgo

El objetivo de esta etapa, es identificar las fuentes de riesgo, zonas de impactos, los acontecimientos y sus causas y sus posibles consecuencias. Para identificar los riesgos primero es necesario identificar los activos y valorar los activos para luego identificar sus vulnerabilidades y amenazas asociadas, en base a esto se han definido los siguientes procesos:

Actividad 1: Identificar activos

Esta etapa consiste en identificar los activos que componen el sistema considerando los activos que dan soporte a los procesos identificados en la etapa anterior y determinando sus características y atributos.

Los activos de una organización son todas aquellas cosas a las que la empresa les da valor (O'Hehir 2002). En ese mismo orden de ideas, debe existir una adecuada gestión de los activos para poder mantener una adecuada protección de los mismos en la empresa (Peltier 2001).

Además de identificar los activos, es necesario clasificarlos de tal manera que se pueda medir de mejor manera su importancia y nivel de

protección. Para ello, se propone la siguiente clasificación de los activos de TI:

- **Procesos del negocio [P]**
  Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados (ISO/IEC 9000).

- **Servicios [S]**
  Conjunto de actividades que buscan responder las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos, potenciando el valor de estos y reduciendo el riesgo inherente del sistema.

- **Software [SW]**
  Programas informáticos diseñados como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas.

- **Hardware [HW]**
  Está conformado por los elementos de hardware que soportan las aplicaciones.

- **Soporte de información [Media]**
  Se consideran los dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Para la identificación de activos de los riesgos se establece la siguiente plantilla:

Tabla 18. Plantilla para la identificación de activos

IDENTIFICACIÓN DE ACTIVOS					CÓDIGO: P007
Elaborado por: _____ Revisado por: _____ Aprobado por: _____					
N°	**CÓDIGO**	**NOMBRE**	**DESCRIPCION**	**RESPONSABLE**	**TIPO**
1	Código del activo	Nombre del activo	Breve descripción del activo	Unidad responsable del activo.	Tipo de activo.

En el caso de las microfinancieras, se pueden identificar de manera genérica los siguientes activos:

Tabla 19. Principales activos en las microfinancieras

N°	CÓDIGO	NOMBRE	DESCRIPCIÓN	RESPONSABLE	TIPO
1	[P_Col]	Proceso de colocación de créditos	Otorgar créditos a las personas, empresas u organizaciones que los soliciten.	Negocios	Procesos del negocio.
2	[P_Cap]	Proceso de captación de fondos	Recolectar dinero de las personas u organizaciones generando intereses a su favor.	Negocios	Procesos del negocio.
3	[P_Rep]	Proceso de cobranza	Recuperar el capital e interés de los créditos otorgados no pagados en los plazos pactados.	Recuperaciones	Procesos del negocio.
4	[P_Acl]	Proceso de atención al cliente	Servicio brindado al cliente a fin que obtenga el producto financiero en el momento y lugar adecuado y se asegure un uso correcto.	Operaciones	Procesos del negocio.
5	[S_Email]	Servicio de	Servicio de	TI	Servicio

Nº	CÓDIGO	NOMBRE	DESCRIPCIÓN	RESPONSABLE	TIPO
		correo electrónico	mensajería instantánea a través de sistemas de comunicación electrónicos.		
6	[S_Internet]	Servicio de acceso a internet	Servicio que permite la interconexión de computadoras para compartir recursos.	TI	Servicio
7	[S_Tel]	Servicio de telefonía	Servicio de comunicación a través de teléfonos celulares y fijos	TI	Servicio
8	[SW_GFin]	Sistema de gestión financiera	Solución empresarial a medida, que permite controlar y supervisar las operaciones de activos y pasivos, relacionadas al negocio financiero.	TI	Software
9	[SW_GAdm]	Sistema de gestión administrativa	Software administrativo y contable.	TI	Software
10	[SW_PWeb]	Página Web	Sirve para mostrar la información de los productos y servicios ofrecidos para cumplir con el principio de transparencia de la información.	TI	Software
11	[HW_SBD]	Servidor de base de datos	Aplicación que permite acceder a base de datos desde terminales o equipos.	TI	Hardware
12	[HW _SApp]	Servidor de aplicaciones	Aplicación que permite acceder a	TI	Hardware

Nº	CÓDIGO	NOMBRE	DESCRIPCIÓN	RESPONSABLE	TIPO
			programas informáticos desde terminales o equipos.		
13	[HW _SRed]	Servidor de red de comunicaciones	Combinación de hardware y software que permite el acceso remoto a herramientas o información que generalmente residen en una red de dispositivos.	TI	Hardware
14	[HW_ECom]	Equipos de cómputo	Conformado por las computadoras personales, dispositivos de almacenamiento, impresoras, etc.	TI	Hardware
15	[HW_SDom]	Servidor de Dominio	Aplicación que permite la administración del sitio web.	TI	Hardware
16	[Media _BD]	Backups de base de datos	Copia de seguridad de las bases de datos completas o parciales.	TI	Soporte de información
17	[Media _App]	Backups de aplicaciones	Copia de seguridad de los sistemas de información.	TI	Soporte de información
…	…	…	…	..	..

Actividad 2: Valorar activos

Esta etapa, consiste en la asignación de un valor que para la organización tiene el activo si llegara a dañarse, perderse o divulgarse, es decir, es la asignación en términos de la importancia, en cuanto a las características de la información:

- **Confidencialidad:** propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos (ISO/IEC 13335-1:2004).

- **Integridad:** propiedad de salvaguardar la precisión y completitud de los activos (ISO/IEC 13335-1:2004).

- **Disponibilidad:** propiedad de estar disponible y utilizable por solicitud de una entidad autorizada (ISO/IEC 13335-1:2004).

- **Cumplimiento Normativo:** capacidad de detectar y gestionar los riesgos de incumplimiento de las obligaciones regulatorias internas y externas, mitigando los riesgos de sanciones y las pérdidas.

Dado que en una organización no todos los activos de información poseen el mismo valor, a la vez que un mismo activo puede poseer un valor diferente para distintas áreas, se establece una valoración estandarizada (1-5) para cada criterio:

Tabla 20. Criterios para evaluar la Confidencialidad

CONFIDENCIALIDAD (C)	VALOR
No aplica.	1
Conocido y/o utilizado sin autorización por cualquier persona, dentro y fuera de la microfinanciera.	2
Conocido y/o utilizado por todo el personal dentro de la microfinanciera.	3
Conocido y/o utilizado por personas que lo necesiten para realizar su trabajo dentro de la microfinanciera.	4
Conocido y/o utilizado estrictamente por personas en particular dentro de la microfinanciera, cuya divulgación podría ocasionar un grave perjuicio.	5

Tabla 21. Criterios para evaluar la Integridad

INTEGRIDAD (I)	VALOR
No aplica.	1
Modificación no autorizada no impide la realización en las actividades de la microfinanciera.	2
Modificación no autorizada genera un impacto insignificativo o menor en las actividades de la microfinanciera.	3
Modificación genera no autorizada un impacto significativo en las actividades de la microfinanciera.	4
Modificación no autorizada impidiendo la realización de las actividades de la microfinanciera.	5

La microfinanciera debe definir qué significa un impacto significativo y no significativo de acuerdo a su realidad.

Tabla 22. Criterios para evaluar la Disponibilidad

DISPONIBILIDAD (D)	VALOR
No aplica.	1
La inaccesibilidad no afecta la actividad normal de la microfinanciera.	2
La inaccesibilidad permanente durante una semana podría impedir la ejecución de las actividades de la microfinanciera.	3
La inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la microfinanciera.	4
La inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la microfinanciera.	5

Tabla 23. Criterios para evaluar la el Cumplimiento Normativo

CUMPLIMIENTO NORMATIVO (N)	VALOR
No aplica.	1
El incumplimiento normativo no ocasiona sanciones y pérdidas significativas para la microfinanciera.	2
El incumplimiento normativo ocasiona una observación sustentable para la microfinanciera.	3
El incumplimiento normativo ocasiona sanciones y pérdidas leves para la microfinanciera.	4
El incumplimiento normativo ocasiona sanciones y las pérdidas graves para la microfinanciera.	5

La microfinanciera debe definir qué significa una falta leve y grave de acuerdo a su realidad.

El valor máximo de las cuatro características determinará la criticidad del activo analizado como se muestra en la siguiente tabla:

Tabla 24. Valoración del nivel de criticidad de activos

VALOR MÁXIMO	NIVEL DE CRITICIDAD
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

En base a cada criterio, es necesario que cada una de las áreas involucradas, valorice los activos según la siguiente plantilla:

Tabla 25. Plantilla para valoración de activos

VALORIZACIÓN DE ACTIVOS							CÓDIGO: P008
Elaborado por: _____ Revisado por: _____ Aprobado por: _____							
N°	ACTIVO	CRITERIOS				TOTAL	NIVEL DE CRITICIDAD
		C	I	D	N		
1	Nombre del activo	Ver Tabla 20	Ver Tabla 21	Ver Tabla 22	Ver Tabla 23	Máximo valor de los criterios	Ver Tabla 24

Actividad 3: Identificar amenazas y vulnerabilidades

En esta etapa, resulta importarte identificar las principales amenazas que explotan las vulnerabilidades de cada activo, para ello se puede partir de la experiencia pasada, propia o de organizaciones similares, considerar el catálogo de amenazas y vulnerabilidades propuesto (Anexo 4). Lo que ha ocurrido puede repetirse y, en cualquier caso, sería impresentable no tenerlo en cuenta. Se propone la siguiente plantilla en donde se plantean las amenazas y vulnerabilidades más frecuentes en el sector financiero.

Tabla 26. Plantilla de identificación de amenazas del sector financiero

IDENTIFICACIÓN DE AMENAZAS			CÓDIGO: P009
Elaborado por: _____ Revisado por: _____ Aprobado por: _____			
N°	ACTIVO	AMENAZA	VULNERABILIDAD
1	Proceso de colocación de créditos	Mal funcionamiento de software	Especificaciones poco claras o incompletas para desarrolladores
2	Proceso de captación de fondos	Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia de acuerdos de niveles de servicio
3	Proceso de cobranza	Abuso de los derechos	Defectos bien conocidos en el software

IDENTIFICACIÓN DE AMENAZAS			CÓDIGO: P009
Elaborado por: _____ Revisado por: _____ Aprobado por: _____			
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**
4	Proceso de atención al cliente	Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador
5	Servicio de correo electrónico	Error en el uso	Falta de políticas de uso de correo electrónico
6	Servicio de internet	Uso no autorizado de equipo	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería
7	Servicio de telefonía	Falta o insuficiencia de provisiones (relativas a seguridad) en contratos con clientes y/o terceras partes	Abuso de privilegios
8	Sistema de gestión financiera	Incumplimiento en el mantenimiento del sistema de información	Falta de procedimiento de control de cambios
9	Sistema de gestión administrativa	Mal funcionamiento del software	Especificaciones incompletas o no claras para los desarrolladores
10	Página Web de la Institución	Mal funcionamiento de software	Falta de control eficaz del cambio
11	Servidor BD	Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información
12	Servidor de aplicaciones	Ataque cibernético	Falta de protección al servidor de aplicaciones web.
13	Servidor de red de comunicaciones	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación
14	Equipos de cómputo	Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico
15	Servidor de dominio	Redirección de pagina	Faltas de mecanismos de seguridad del DNS
16	Backup de base de datos	Destrucción de equipo o medios	Procedimientos inadecuados de reclutamiento
...	...	...	...

Fase IV: Análisis del riesgo

Esta fase, tiene como objetivo determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. Según esto se establecen los siguientes procesos:

Actividad 1: Definir criterios del riesgo

En las siguientes tablas se establecen los criterios de valoración de cada variable:

Tabla 27. Valoración de probabilidad de ocurrencia

VALOR	PROBABILIDAD [P]	DESCRIPCIÓN
1	Raro	Puede ocurrir en circunstancias excepcionales 1 vez cada 5 años.
2	Improbable	Se podría presentar una vez cada 5 años.
3	Posible	Se podría presentar una vez al año.
4	Probable	Se podría presentar una vez cada mes.
5	Casi seguro	Se podría presentar varias veces en el mes.

Los tiempos establecidos se obtuvieron a partir del análisis de 3 microfinancieras.

Tabla 28. Valoración de Impacto

VALOR	IMPACTO [I]	DESCRIPCIÓN
1	Insignificante	Tiene un efecto nulo o muy pequeño en las operaciones.
2	Menor	Afecta parcialmente las operaciones.
3	Moderado	Operativamente es sostenible, pero dificulta o retrasa las operaciones.
4	Mayor	Paraliza la atención de servicios críticos a clientes, debido a la caída significativa de las operaciones.
5	Catastrófico	Paraliza todas las operaciones de la entidad.

En base a la determinación de la probabilidad y la valoración del impacto, se establecen los niveles de riesgos según la siguiente clasificación semaforizada:

Tabla 29. Nivel de riesgo

RANGO	NIVEL DE RIESGO	DESCRIPCIÓN
1 – 5	1	Bajo
6 – 10	2	Medio
11 – 15	3	Alto
16 – 25	4	Extremo

Para determinar la probabilidad e impacto de cada riesgo debe tomar como referencia la información histórica y las políticas de riesgos de la microfinanciera, en caso no contar con esta información puede basarse en los valores promedio del sector.

Actividad 2: Estimar el riesgo

El riesgo es la combinación de la probabilidad de un evento y su ocurrencia (ISO/IEC Guía 73:2002). Por tanto, para determinar el nivel de criticidad es necesario analizarlo mediante la determinación de ambos factores:

$$\text{Riesgo} = \text{Impacto} \times \text{Probabilidad}$$

Para el estimar el riesgo que implica cada amenaza, se propone la siguiente plantilla:

Tabla 30. Plantilla de análisis de riesgos

<table>
<tr><th colspan="8">ANÁLISIS DE RIESGOS</th><th>CÓDIGO: P010</th></tr>
<tr><td colspan="9">Elaborado por: _____
Revisado por: _____
Aprobado por: _____</td></tr>
<tr><th rowspan="2">N°</th><th rowspan="2">ACTIVO</th><th rowspan="2">AMENAZA</th><th rowspan="2">VULNERABILIDAD</th><th rowspan="2">P</th><th rowspan="2">I</th><th rowspan="2">PxI</th><th colspan="2">RIESGO</th></tr>
<tr><th>CÓDIGO</th><th>NIVEL</th></tr>
<tr><td rowspan="5">1</td><td rowspan="5">Nombre del activo</td><td rowspan="2">Amenaza 1.1</td><td>Vulnerabilidad 1.1.1</td><td rowspan="5">Ver Tabla 27</td><td rowspan="5">Ver Tabla 28</td><td rowspan="5">Probabilidad x Impacto</td><td rowspan="5">Código del Riesgo</td><td rowspan="5">Ver Tabla 29</td></tr>
<tr><td>Vulnerabilidad 1.1.2</td></tr>
<tr><td rowspan="3">Amenaza 1.2</td><td>Vulnerabilidad 1.2.1</td></tr>
<tr><td>Vulnerabilidad 1.2.2</td></tr>
<tr><td>Vulnerabilidad 1.2.3</td></tr>
</table>

Fase V: Evaluación del riesgo

La evaluación del riesgo, es el proceso de comparación de los resultados del análisis del riesgo, con sus criterios, para determinar si el riesgo o su magnitud son aceptables o tolerables. (ISO/IEC Guía 73:2002).
Esta fase consta de dos procesos:

Actividad 1: Priorizar riesgos

Una matriz de calor permitirá priorizar los riesgos identificados, según el impacto y probabilidad se definirá la ubicación del riesgo dentro de la matriz facilitando identificar la prioridad del riesgo lo que facilitará luego toma de decisiones de la opción de tratamiento más adecuada.

En la siguiente figura, se muestra el mapa de calor propuesto para el caso de las empresas microfinancieras donde se muestran las prioridades que debe tener cada riesgo según donde se ubique.

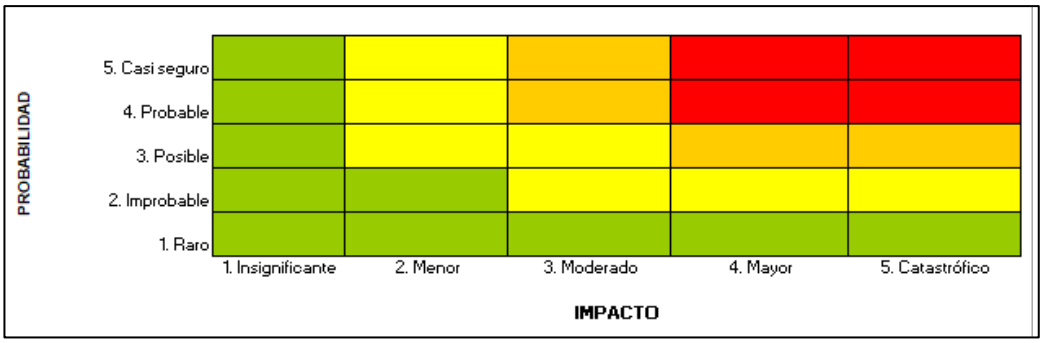


Figura 11. Mapa de calor

El mapa de calor, se representa en formato de matriz con dos ejes. En las ordenadas, la probabilidad de ocurrencia y, en el de las abscisas, el impacto que un riesgo tendría si se materializa.

Para ubicar un riesgo dentro de la matriz, considerar los puntajes establecidos para la probabilidad e impacto en la fase anterior. Según esto, el riesgo se ubica en la zona verde, amarilla, naranja o roja indicando el nivel de riesgo: bajo, medio, alto, extremo respectivamente.

Actividad 2: Valorar riesgos

Sabiendo el nivel de prioridad que tiene cada riesgo, es necesario conocer el apetito y la tolerancia establecidos para cada uno según el contexto y los procesos de negocio a los que afecta.

Según ISACA en la publicación de COBIT 5 (2012) se definen los siguientes conceptos:

- **Apetito de riesgo:** nivel de riesgo en diferentes aspectos que una empresa está dispuesta a aceptar en pos del cumplimiento de su misión (o visión).

- **Tolerancia de riesgo:** nivel aceptable de variación que la gerencia está dispuesta a permitir para un riesgo en particular, en el cumplimiento de sus objetivos.

El producto del impacto y la probabilidad del riesgo (M), debe ser comparada con el apetito (A) y tolerancia (T) para determinar si es riesgo es *Aceptable*, *Tolerable* o *Intolerable* según la siguiente tabla:

Tabla 31. Valorización de riesgos

CONDICIÓN	VALORIZACIÓN
M < A	Aceptable
M >= A y M =< T	Tolerable
M > T	Intolerable

Para la valorización de los riesgos se establece la siguiente plantilla:

Tabla 32. Plantilla de Valorización de riesgos

<table>
<tr><th colspan="8">VALORIZACIÓN DE RIESGOS</th><th>CÓDIGO: P011</th></tr>
<tr><td colspan="9">Elaborado por: _____
Revisado por: _____
Aprobado por: _____</td></tr>
<tr><th colspan="2">RIESGO</th><th rowspan="2">ACTIVO</th><th rowspan="2">AMENAZA</th><th rowspan="2">VULNERABILIDAD</th><th rowspan="2">PXI</th><th rowspan="2">APETITO</th><th rowspan="2">TOLERACIA</th><th rowspan="2">VALORIZACIÓN</th></tr>
<tr><th>CÓDIGO</th><th>NIVEL</th></tr>
<tr><td rowspan="5">Código del Riesgo</td><td rowspan="5">Ver Tabla 29</td><td rowspan="5">Nombre del Activo</td><td rowspan="2">Amenaza 1.1</td><td>Vulnerabilidad 1.1.1</td><td rowspan="5">Probabilidad x Impacto</td><td rowspan="5">Valor de apetito de riesgo</td><td rowspan="5">Valor de tolerancia al riesgo</td><td rowspan="5">Ver Tabla 31</td></tr>
<tr><td>Vulnerabilidad 1.1.2</td></tr>
<tr><td rowspan="3">Amenaza 1.2</td><td>Vulnerabilidad 1.2.1</td></tr>
<tr><td>Vulnerabilidad 1.2.2</td></tr>
<tr><td>Vulnerabilidad 1.2.3</td></tr>
</table>

Fase VI: Tratamiento del riesgo

El tratamiento del riesgo consiste en seleccionar una o más opciones de modificación de los riesgos, y la aplicación de esas opciones. Una vez en marcha, los tratamientos de proporcionar o modificar los controles existentes. (ISO/IEC 31000:2009).

Actividad 1: Seleccionar estrategias de tratamiento

Para esta metodología se tomará lo propuesto en el estándar ISO/IEC 27005:2005 en el que se definen las estrategias de tratamiento de la siguiente manera:

- **Reducir los riesgos:** Tomar medidas necesarias, para disminuir el impacto y probabilidad del riesgo, generalmente se logra con la implementación de controles, mejoramiento de actividades, monitoreo constante, etc.

- **Retener los riesgos:** Retener el riesgo significa que los daños ocasionados por su materialización no son significativos, generalmente se establecen planes de acción y mejora, provisión de recursos, etc.

- **Evitar los riesgos:** Tomar medidas necesarias para prevenir la materialización del riesgo, si es viable, generalmente se logra con cambios en los procesos, implementación de controles, establecimiento de nuevas política, etc.

- **Transferir los riesgos:** Se reduce el efecto del riesgo a través del traspaso de las pérdidas a otras organizaciones, como en el caso de contratos de seguros.

Las vulnerabilidades, con las amenazas asociadas indican donde la protección pudiera ser requerida con mayor prioridad y según eso se selecciona la estrategia de tratamiento a implementar, para lo cual se debe completar la siguiente plantilla:

Tabla 33. Plantilla de tratamiento de riesgos

<table>
<tr><th colspan="6">TRATAMIENTO DE RIESGOS</th><th>CÓDIGO: P012</th></tr>
<tr><td colspan="7">Elaborado por: _____
Revisado por: _____
Aprobado por: _____</td></tr>
<tr><th colspan="2">RIESGO</th><th rowspan="2">ACTIVO</th><th rowspan="2">AMENAZA</th><th rowspan="2">VULNERABILIDAD</th><th rowspan="2">VALORIZACIÓN</th><th rowspan="2">ESTRATEGIA</th></tr>
<tr><th>CÓDIGO</th><th>NIVEL</th></tr>
<tr><td rowspan="5">Código del Riesgo</td><td rowspan="5">Ver Tabla 29</td><td rowspan="5">Nombre del activo</td><td rowspan="2">Amenaza 1.1</td><td>Vulnerabilidad 1.1.1</td><td rowspan="5">Ver Tabla 31</td><td rowspan="5">Según la clasificación propuesta</td></tr>
<tr><td>Vulnerabilidad 1.1.2</td></tr>
<tr><td rowspan="3">Amenaza 1.2</td><td>Vulnerabilidad 1.2.1</td></tr>
<tr><td>Vulnerabilidad 1.2.2</td></tr>
<tr><td>Vulnerabilidad 1.2.3</td></tr>
</table>

Actividad 2: Proponer planes de acción

Una vez identificada la estrategia de tratamiento de cada riesgo, se deben tomar acciones para llevar al riesgo a un nivel aceptable para la organización. Los planes de acción serán generados para los riesgos que presenten los niveles extremo y alto, sin embargo se podrán establecer planes de acción adicionalmente, para riesgos de menores niveles, si se requiere reducir el nivel del riesgo.

Los planes de acción, que muestren atraso en su plazo de implementación o que no puedan ser implementados, por razones externas a las áreas o unidades de negocio, deberán de justificar los mismos e implementar mitigantes temporales de los riesgos detectados, debiendo de tener la aprobación de su gerencia o jefatura inmediata superior en primera instancia.

En la siguiente plantilla, se establecen los criterios que se deben contemplar para plantear un plan de acción.

Tabla 34. Plantilla para plan de acción

PLAN DE ACCIÓN	**CÓDIGO: P013**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____	
NOMBRE DEL PLAN DE ACCION	
Descripción	Describir cual es el propósito del plan para la empresa microfinanciera.
Alcance	Describir cuales son las actividades que abarcan el plan para la empresa.
Objetivos	Describir los objetivos del plan y su aplicación en la empresa.
Roles, responsabilidades y autoridades	Describir los roles que conforman el equipo de recuperación y las responsabilidades que tiene cada uno.
Riesgos asociados	Mencionar los riesgos asociados a este plan de acción.

PLAN DE ACCIÓN		CÓDIGO: P013
Nivel del riesgo	Describir el nivel del riesgo.	
Aplicaciones de los procesos	Describir las aplicaciones que utilizan los procesos críticos para su normal operatividad y los módulos que estos utilizan.	
Registros vitales	Describir toda aquella información necesaria para realizar la recuperación de los servicios de TI como manuales, contraseñas, configuraciones, etc.	
Recursos necesarios	Describir todos los equipos, servidores y mecanismos de comunicación para el restablecimiento de los servicios de TI.	
Procedimiento de recuperación ante emergencias	Describir el paso a paso de las actividades a seguir para realizar la recuperación de los servicios de TI.	
Indicador clave de riesgo	Definir indicadores que permitan medir la efectividad del plan de acción.	

El siguiente recuadro muestra las acciones a seguir para las amenazas mapeadas en este modelo

Tabla 35. Planes de acción sugeridos según amenazas mapeados

ACTIVO	AMENAZA	VULNERABILIDAD	PLAN DE ACCIÓN
Proceso de colocación de créditos	Mal funcionamiento de software	Especificaciones poco claras o incompletas para desarrolladores	Actualización de contratos y/o adendas
Proceso de captación de fondos	Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia de acuerdos de niveles de servicio	
Proceso de cobranza	Abuso de los derechos	Defectos bien conocidos en el software	
Proceso de atención al cliente	Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador	Procedimiento de monitoreo de ejecución de procesos nocturnos
Servicio de correo electrónico	Error en el uso	Falta de políticas de uso de correo electrónico	Reforzar políticas de uso de medios de telecomunicación y mensajería
Servicio de internet	Uso no autorizado de equipo	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería	

ACTIVO	AMENAZA	VULNERABILIDAD	PLAN DE ACCIÓN
Servicio de telefonía	Falta o insuficiencia de provisiones (relativas a seguridad) en contratos con clientes y/o terceras partes	Abuso de privilegios	Actualización de contratos y/o adendas
Sistema de gestión financiera	Incumplimiento en el mantenimiento del sistema de información	Falta de procedimiento de control de cambios	Procedimiento de control de cambios
Sistema de gestión administrativa	Mal funcionamiento del software	Especificaciones incompletas o no claras para los desarrolladores	Mecanismo para asegurar claridad en documento de especificaciones
Página Web de la Institución	Mal funcionamiento de software	Falta de control eficaz del cambio	reforzar equipo de control de calidad para pruebas de software
Servidor BD	Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	Actualización de la política de acceso
Servidor de aplicaciones	Ataque cibernético	Falta de protección al servidor de aplicaciones web.	Elaboración de procedimientos en defensa de ciberataques
Servidor de red de comunicaciones	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación	reforzar la seguridad física
Equipos de computo	Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	Mantenimiento de equipos
Servidor de Dominio	Redirección de pagina	Faltas de mecanismos de seguridad del DNS	Elaborar mecanismos de seguridad para el servidor de dominio
Backup de base de datos	Destrucción de equipo o medios	Procedimientos inadecuados de reclutamiento	Capacitación al personal
...	...	...	...

En la siguiente plantilla se plantea una matriz para hacer seguimiento a los planes de acción planteados.

Tabla 36. Plantilla para seguimiento de planes de acción

SEGUIMIENTO DE PLANES DE ACCIÓN						**CÓDIGO: P014**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____						
RIESGO		**PLAN DE ACCIÓN**	**DESCRIPCIÓN**	**PRESUPUESTO ASIGNADO**	**FECHA OBJETIVO**	**RESPONSABLE**
CÓDIGO	**NIVEL**					
Código del Riesgo	Ver Tabla 30	Plan 1.1.1	Descripción del plan de acción	Monto presupuestado	Fecha estimada de término	Persona o área responsable

Fase VII: Monitoreo y revisión

En este proceso, se realiza una revisión continua del desempeño y avance de la metodología aplicada para la gestión de riesgos. Se recomienda hacer la revisión del proceso de gestión de riesgos por lo menos una vez al año.

El monitoreo externo de la gestión de riesgos de TI, es efectuado por las auditorías externas: SBS y AFP, ASOMIF, entre otros que se realicen y permitirán la retroalimentación.

El monitoreo interno de la gestión de riesgos de TI será realizado por la unidad de riesgos y la unidad de auditoría interna, y para dicho efecto se coordinará con las áreas pertinentes a fin de verificar que las medidas de tratamiento vienen siendo implementadas adecuadamente.

Esta fase se centra principalmente en evaluar los planes de acción propuestos en la fase anterior, para ello se plantea la siguiente plantilla:

Tabla 37. Ficha de monitoreo y revisión

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P015
Elaborado por: _____ Revisado por: _____ Aprobado por: _____									
RIESGO		**PLAN DE ACCIÓN**	**DESCRIPCIÓN**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
Código del Riesgo	Ver Tabla 29	Plan 1.1.1	Descripción del plan de acción	Fecha estimada de término	Fecha real de culminación	Persona o área responsable	Monto presupuestado	Monto real gastado	Pendiente, Concluido o en Ejecución.

Fase VII: Comunicación y consulta

Es indispensable, contar con la participación de todas las unidades de la empresa, para comunicar permanentemente al área de riesgos la ocurrencia de incidentes o eventos relacionados a TI que afecten a la organización. El área de riesgos debe ser capaz de relacionarse rápidamente con las unidades de negocios y concientizar a los trabajadores a través de estas unidades. Uno de los aspectos a considerar es que todas las áreas de la empresa deberán de comunicar mediante los medios establecidos por la empresa, los incidentes que se originen de acuerdo a la siguiente plantilla.

Tabla 38. Plantilla de comunicación y consulta

COMUNICACIÓN DE RIESGOS Y CONSULTAS		**CÓDIGO: P016**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
TIPO DE COMUNICACIÓN	Factor de riesgo	Mejora
COMUNICANTE		
NOMBRE	Nombres completos del comunicante.	
OFICINA	Oficina o área a la que pertenece el comunicante.	
FECHA	Fecha de la comunicación	
DETALLE	Indicar detalladamente el incidente o situación de mejora encontrada.	
DOCUMENTOS ADJUNTOS	Listar los documentos que se adjuntan como parte de las evidencias.	

1.4 Evaluación de indicadores

Para contrastar la hipótesis se evaluarán los siguientes indicadores:

1.4.1 Armonización de las metodologías, estándares y normas de gestión de riesgos de TI.

Para el desarrollo del método de gestión de riesgos se han tomado en cuenta principalmente dos aspectos:

- Normativas SBS relacionadas a la gestión de riesgos: reglamento para la gestión del riesgo operacional (Resolución S.B.S. N° 2116-2009), gestión de la continuidad del negocio (Circular G-139-2009) y gestión de la seguridad de la información (Circular G-140-2009).

- Estándares y metodologías: ISO/IEC 31000, ISO/IEC 27005, ISO 22301, OCTAVE, MAGERIT, COBIT 5 para Riesgos.

Con relación a estos dos aspectos, se recopiló la información de las metodologías teniendo en cuenta la estructura que cada uno plantea para abordar la gestión de riesgos y se revisaron las normativas para que el modelo planteado pueda darles cumplimiento.

En el siguiente gráfico se muestra lo que se ha tomado de cada uno de los estándares y metodologías:

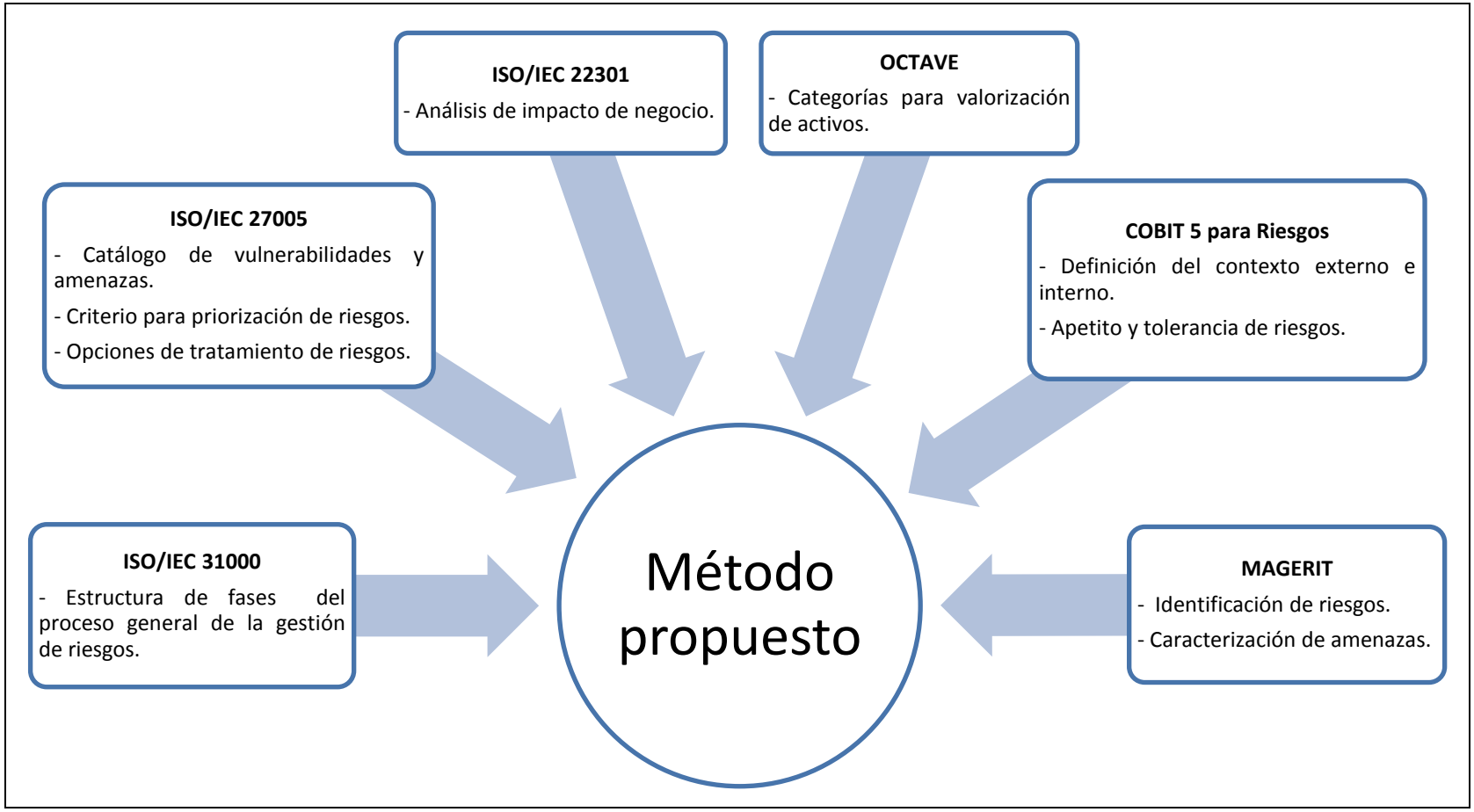


Figura 12. Esquema de método de gestión de riesgos propuesto para microfinancieras

1.4.2 Impacto de negocio en los procesos esenciales para el sector microfinanciero.

Según el análisis realizado en la aplicación del método (Anexo 7 - Fase II), se han identificado que el 44% lo conforman los macro-procesos críticos. Lo conforman los macro-procesos de gestión comercial, captaciones, colocaciones y recuperaciones. Estos macro-procesos tienen un alto impacto financiero, dado que generan ingresos a la organización y en donde la interrupción del sistema podría ocasionar perdidas a grandes escalas. Además tienen un alto impacto regulatorio, dado que son monitoreados constantemente por la SBS.

El 22% lo conforman los macro-procesos vitales, si bien no son procesos que aportan ganancias a la organización, ayudan y dan soporte a los procesos críticos dado que consolidan información o administran las operaciones.

El 33% lo conforman los macro-procesos sensibles. Estos son procesos procedimentales, es decir no necesitan que el sistema esté disponible para desarrollarse.

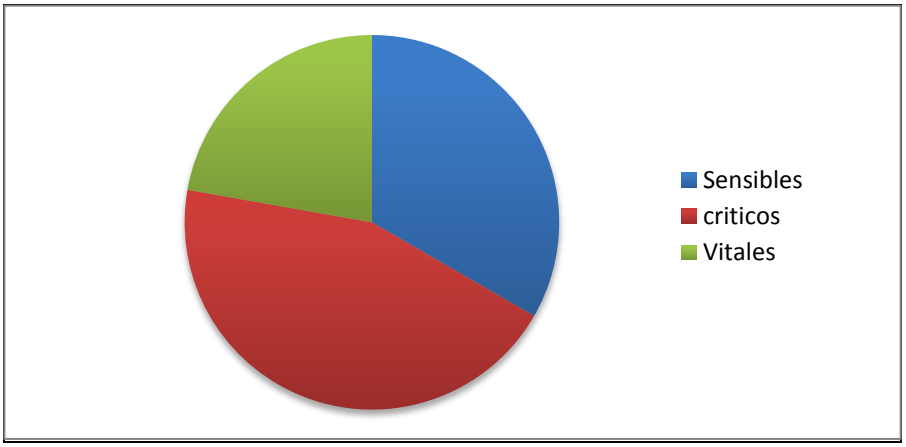


Figura 13. Clasificación de procesos en microfinancieras

1.4.3 Validez del modelo de gestión de riesgos de TI en microfinancieras.

Para probar la validación del modelo se usaron dos métodos.

El primer método consistió en someter al modelo a una evaluación por juicio de expertos donde se seleccionaron a 3 profesionales (k = 3) con amplia trayectoria en la gestión de riesgos. Basado en lo propuesto por Escobar y Cuervo, se formuló un formato para validación de expertos del modelo propuesto (Anexo 5) con el fin de recoger la opinión de los especialistas respecto a la suficiencia, realidad, coherencia y relevancia de cada una de las actividades que contempla el modelo (N = 17).

Para evaluar el acuerdo entre las respuestas de los expertos (Anexo 6), se usó el coeficiente de concordancia W de Kendall con un nivel de significancia de 0.05, es decir con 95% de confianza. Este estadístico sigue una distribución chi-cuadrada (χ^2) con N – 1 grados de libertad.

El coeficiente de concordancia de Kendall puede variar de 0 a 1, mientras mayor sea el valor de Kendall entonces más fuerte será la concordancia. A partir de esto se plantean dos hipótesis:

- H_0: No existe concordancia entre las opiniones de los evaluadores (W = 0).
- H_1: Existe concordancia entre las opiniones de los evaluadores (W > 0).

Usando el programa estadístico SPSS para evaluar la concordancia de cada uno de los criterios considerados en el juicio de expertos, se obtuvieron los siguientes resultados:

Tabla 39. Estadístico de prueba W de Kendall

	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
N	17	17	17	17
W	0.381	0.607	0.381	0.474
$\chi 2$	12.943	20.642	12.943	16.128
gl	2	2	2	2
p	0.002	0.000	0.002	0.000

Según los resultados de la tabla anterior, como en cada uno de los criterios es valor de W es mayor que cero, se rechaza la hipótesis nula y se concluye que existe concordancia entre las opiniones de los evaluadores con respecto a la suficiencia, claridad, coherencia y relevancia y es valor de $p < 0.05$ es significativo.

Para demorar la confiabilidad del instrumento usado para el diagnóstico del contexto microfianciero, se usó el coeficiente alfa de Cronbach, obteniendo el siguiente resultado:

Tabla 40. Estadístico de confiabilidad Alfa de Cronbach

ALFA DE CRONBACH	ALFA DE CRONBACH BASADOS EN ELEMENTOS ESTANDARIZADOS	N ELEMENTOS
0.621	0.621	30

Considerando lo especificado por Herrera (1998) los valores hallados pueden ser comprendidos entre la siguiente tabla:

Tabla 41. Valores para estimar el nivel confiabilidad

VALOR	CONCLUSIÓN
0,53 a menos	Confiabilidad nula
0,54 a 0,59	Confiabilidad baja
0,60 a 0,65	Confiable
0,66 a 0,71	Muy Confiable
0,72 a 0,99	Excelente confiabilidad
1.0	Confiabilidad perfecta

En base a la tabla anterior, se puede considerar que el coeficiente de confiabilidad obtenido es confiable.

1.4.4 Formulación del esquema estándar para planes de acción de TI.

Según el análisis realizado sobre los riesgos de TI comunes que están presentes constantemente en las instituciones microfinancieras, se ha estimado que los principales riesgos están presentes en los sistemas de información, equipos tecnológicos y base de datos:

Tabla 42. Riesgos tecnológicos

ACTIVO	AMENAZA	VULNERABILIDAD
Sistemas de información de la empresa	Incumplimiento en el mantenimiento del sistema de información	Falta de procedimiento de control de cambios.
	Error en el uso	Falta de capacitación a los usuarios.
	Procesamiento ilegal de los datos	Falta de mecanismos de monitoreo.
Equipos informáticos	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.
	Falsificación de derechos	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.
Base de datos	Manipulación con software	Falta de copias de respaldo.
	Falsificación de derechos	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.

El 40% son los riesgos relacionados a los sistemas de información, el 30% están relacionados a los riesgos presentes en los equipos informáticos y el otro 30% relacionado a los riesgos presentes en el manejo y administración de las bases de datos.

En base a este análisis se han identificado los siguientes planes de acción para preservar la continuidad del negocio, como se sugiere en la circular G-139-2009:

- **Plan de recuperación de servicios de TI**: Este plan del sistema de gestión de continuidad del negocio tiene como objetivo restaurar en el menor tiempo posible los sistemas de información que soportan los procesos críticos del negocio.

- **Plan de crisis:** Este plan del sistema de gestión de continuidad del negocio tiene como objetivos principales establecer los procedimientos a seguir, definir y asignar responsabilidades, definir los canales de comunicación oportunos y preservar la reputación de la empresa.

- **Plan de entrenamiento y capacitación para el personal de la organización:** tiene como objetivo principal el establecimiento de un programa de capacitación y entrenamiento del personal de la empresa.

Plantilla propuesta para planes de acción:

Tabla 43. Plantilla estándar para formulación de planes de acción

PLAN DE ACCIÓN	**CÓDIGO: P013**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____	
PLAN DE RECUPERACIÓN DE SERVICIOS DE TI	
Descripción	
Alcance	

PLAN DE ACCIÓN	CÓDIGO: P013
Elaborado por: _____ Revisado por: _____ Aprobado por: _____	
PLAN DE RECUPERACIÓN DE SERVICIOS DE TI	
Objetivos	
Roles, responsabilidades y autoridades	
Riesgos asociados	
Nivel del riesgo	
Aplicaciones de los procesos	
Registros vitales	
Recursos necesarios	
Procedimiento de recuperación ante emergencias	
Indicador clave de riesgo	

1.5 Evaluación de la implementación del método

Para validar el modelo propuesto es necesaria su aplicación, donde se seleccionó a 1 de las 3 microfinancieras en estudio para desarrollar cada una de las fases propuestas (Anexo 7) con lo cual se demuestra que el modelo es aplicable a un entorno real.

Adicionalmente, se ha considerado diseñar un cuestionario en base a los indicadores identificados con la finalidad de probar la efectividad del

diseño y de la operación del modelo propuesto determinando si está operando tal como fue diseñado.
Este cuestionario ha sido enviado a un panel de personas seleccionadas de la microfinanciera, para asignar pesos a los factores y variables del modelo propuesto.

Para cada uno de los cuestionarios se utilizará la siguiente tabla de referencia para calificar los pesos de cada una de los indicadores de cada variable:

Tabla 44. Pesos para la calificación de los indicadores

PESO	SIGNIFICADO	
1	Clave	El indicador evaluado del modelo propuesto es importante considerarlo en el sistema de gestión de riesgos de TI de la financiera, porque cumple con los requisitos exigidos en la normativa la SBS y se adecúa a las funciones de la entidad.
2	Relevante	El indicador evaluado del modelo propuesto puede considerarse en el sistema de gestión de riesgos de TI de la financiera, porque cumple con los requisitos exigidos en la normativa la SBS.
3	Estándar	El indicador evaluado del modelo propuesto puede considerarse en el sistema de gestión de riesgos de TI de la financiera, con algunas modificaciones y mejoras para cumplir con los requisitos exigidos en la normativa la SBS y para que se adecúe a las funciones de la entidad.
4	Irrelevante	El indicador evaluado del modelo propuesto no cumple con los requisitos exigidos en la normativa la SBS por lo que no podría considerase en el sistema de gestión de riesgos de TI de la financiera.

En la siguiente tabla se muestra el resultado de la validación de la aplicación evaluada por los involucrados en la gestión de riesgos de TI.

Tabla 45. Resultado de la validación de la aplicación del modelo propuesto

			GERENTE DE TI		SUBGERENTE DE TI		OFICIAL DE SEGURIDAD		GERENTE DE RIESGO OPERACIONAL		OFICIAL DE CONTINUIDAD DEL NEGOCIO		TOTALES	
VARIABLES	**INDICADORES**	**PREGUNTAS**	**SI/NO**	**PESO**	**SI/NO**	**PESO**	**SI/NO**	**PESO**	**SI/NO**	**PESO**	**SI/NO**	**PESO**	**SI/NO**	**PESO**
Continuidad del Negocio	Nivel de armonización de las metodologías, estándares y normas de gestión de riesgos de TI.	¿Se ha determinado el nivel de armonización adecuado y este se refleja en el método propuesto?	SI	2	SI	2	SI	2	SI	2	SI	2	100%	2
	Nivel del impacto de negocio en los procesos esenciales para el sector microfinanciero.	¿Se ha realizado un correcto análisis de impacto de negocio que permita reconocer los procesos esenciales para la continuidad del negocio?	SI	2	SI	2	SI	2	NO	4	SI	3	80%	3
	Nivel de utilidad del modelo de gestión de riesgos de TI en microfinancieras.	¿Se reconoce la utilidad del modelo propuesto para la gestión de riesgos de TI en microfinancieras?	SI	2	SI	2	SI	2	NO	4	SI	2	80%	2
	Nivel de aceptación del esquema estándar para la formulación de planes de acción de TI.	¿Es aceptable el esquema estándar propuesto para la formulación de planes de acción de TI?	SI	1	SI	1	SI	1	SI	2	SI	2	100%	1
TOTALES			100%		100%		100%		50%		100%		90%	2

Con los resultados obtenidos, desde el punto de vista del diseño del modelo propuesto, se puede concluir lo siguiente:

- Aceptan en un 90% de los factores considerados en el método propuesto para la gestión de riesgos de TI y contribuir con la continuidad del negocio, estableciendo que tiene un nivel de madurez RELAVANTE, es decir, que el método propuesto puede considerarse como parte del sistema de gestión de riesgo de la financiera.
- Aceptan en un 100% el factor considerado para el nivel de armonización de las metodologías, estándares y normas de gestión de riesgos de TI, estableciendo que tienen un nivel de madurez RELEVANTE.

Desde el punto de vista de la implementación en la microfinanciera del modelo propuesto, se concluye lo siguiente:

- Aceptan en un 80% el nivel de impacto de negocio de los procesos esenciales para el sector microfinanciero, estableciendo que tiene un nivel de madurez ESTANDAR, es decir el indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Gestión de riesgos de TI de la financiera, con algunas modificaciones y mejoras.

- Aceptan en un 100% el esquema estándar para la formulación de planes de acción de TI, estableciendo que tiene un nivel de madurez CLAVE, es decir, el indicador evaluado del modelo propuesto es importante considerarlo en el Sistema de Gestión de riesgos de TI de la financiera, porque cumple con los requisitos exigidos en la normativa la SBS y se adecúa a las funciones de la entidad.

CONCLUSIONES

Se ha logrado proponer un modelo de gestión de riesgo de TI basado en la armonización de los estándares y metodologías seleccionados para el contexto microfinanciero. A pesar que esta investigación no es la primera en armonizar metodologías de riesgos de TI, solo se tiene un antecedente de una propuesta de método aplicado a las microfinancieras realizada hace 5 años que no abarca todas las etapas propuestas en la ISO/IEC 31000.

Dentro del método propuesto se ha considerado una etapa del análisis de impacto de negocio con el fin de identificar los procesos críticos y en base a dichos procesos obtener los riesgos de TI para aplicar los planes de acción necesarios que garanticen la continuidad del negocio.

A través del juicio de expertos se ha validado la propuesta del método de gestión de riesgos aplicado a microfinancieras de la región Lambayeque obteniendo su aceptación, lo que certifica que el modelo tiene validez para ser aplicado en el contexto microfinanciero.

En base al análisis de los riesgos, se ha logrado obtener una plantilla estándar de los planes de acción que contiene todos los parámetros necesarios para la gestión de riesgos de TI en el contexto microfinanciero.

REFERENCIAS BIBLIOGRÁFICAS

Alexander, Alberto G. *Nuevo estandar internacional de continuidad del negocio*. 2012.

Alvarez Sosa, Yenny Maribel. *Diseño de una Metodologia para el Analisis de Riesgo en los Sistemas de Gestión de Seguridad de Informacion en las Universidades de Barquisimeto Estado Lara (Marisgsi)*. 2013.

Belaunde, Gregorio. El proceso crediticio: una mirada panorámica. 2012.

Berrospi Liu, Ana Claudia, y César Alfredo Valencia Zuñiga. *Análisis y diseño de la arquitectura de procesos de una microfinanciera - procesos de riesgo operacional*. 2013.

Brigham, Eugene, y Joel Houston. *Fundamentos de administración Financiera*. 2005.

Castro, Mauricio. *El Nuevo Estándar para la Gestión de Riesgos*. 2010.

Celi, Ernesto. *Un modelo para la gestión de riesgos de TI en las empresas microfinancieras: caso Lambayeque, Perú*. 2015.

Condori, Gladys Macedo. *Seminario Taller Gestion Del Sistema Financiero*. 2014.

Crespo Rin, Maria del Carmen. *El Análisis de Riesgos dentro de una Auditoría Informática: Pasos y Posibles Metodologías*. 2013.

Escobar Pérez, Jazmine, y Ángela Cuervo Martínez. *Validez de contenido y juicio de expertos*. 2008.

Fernández, José Manuel Ballester. *Gobierno Corporativo TIC*. 2009.

Gobierno de España, Ministerio de Hacienda y Administraciones Publicas.

MAGERIT-v.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2012.

Gómez, Ricardo, Diego Hernán Pérez, Yezid Donoso, y Andrea Herrera. *Metodología y gobierno de la gestión de riesgos de tecnologías de la información*. 2010.

Guirado, Rodrigo. *Gestión de Riesgos y Continuidad Operativa en IT: Recomendaciones Prácticas*. 2015.

Ibarra, José Ángel Peña. *Metodologías y Normas para el Análisis de Riesgos: ¿Cuál debo aplicar?*. 2010.

IBM. *Guía para los Directores de TI (CIOs) en la gestión de riesgos de TI: aprovechar el extraordinario potencial para el valor Guía para los Directores de TI (CIOs) en la gestión de riesgos de TI*. 2008.

INEI. *Panorama de la economía peruana*. 2016.

Iparraguirre Vergara, Juan Carlos, y Saavedra Macedo. *Análisis y diseño de la Arquitectura de procesos de una microfinanciera procesos de captaciones, colocaciones y riesgo*. 2011.

ISACA. *Cobit 5 - Un Marco de Negocio para el Gobierno y la Gestión de la Empresa*. 2012.

ISACA. *Cobit 5 para Riesgos*. 2013.

Norma Internacional ISO/IEC 13335-1. 2004.

Norma Internacional ISO/IEC 27001. 2005.

Norma Internacional ISO/IEC 27005. 2008.

Norma Internacional ISO/IEC 31000. 2009.

Norma Internacional ISO/IEC 9000.

Norma Internacional ISO/IEC Guía 73. 2002.

Lovelock, C. 2009.

Mogollón, Abraham. *Análisis Comparativo: Metodologías de análisis de Riesgos*. 2015.

Muñoz, I., & Ulloa, G. Gobierno de TI – Estado del arte. 2011.

O'Hehir. 2002.

Ochoa, Blanca Rubiela Duque. *Metodologías de Gestión de Riesgos*. 2010.

Pardo Calvache, César Jesús. *Armonización de Múltiples Modelos para el Gobierno de TI y el Desarrollo de Software*. 2012.

Peltier. 2001.

Rodríguez, Norma L., y Carlos G. Herrera. *Validación y Confiabilidad de in instrumento de medición para carreras ed ingeniría*. 2008.

S., Andrés Cheng C. Santiago Pinilla M. Juan D. Villa C. Andrea Herrera. *Riesgo de TI en la banca*. 2014.

Superintendencia de Banca, Seguros y AFP. *Circular G-139-2009*. 2009.

Superintendencia de Banca, Seguros y AFP. *Reglamento de Riesgo Operacional* . 2008.

Superintendencia de Banca, Seguros y APF. *Circular G-105-2002 Riesgos de tecnología de Informacion*. 2002.

Superintendencia de Banca, Seguros y AFP. *Reglamento de la Gestión Integral del Riesgo*. 2008.

Superintendencia de Banca, Seguros y AFP. *Reglamento para la Gestión del Riesgo Operacional*. 2009.

Troitiño, Marina Touriño. *Cobertura del Riesgo Tecnológico: hacia una Auditoría Interna de TI Integrada*. 2014.

Vásquez, Karina del Rocío Gaona. *Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos De La Seguridad De La Información Aplicada a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala*. 2013.

Yépez, Andrés Gustavo Aguayo. *Adaptación de un Marco Metodólogico para la Medición del Riesgo Operativo Generado por Puntos Vulnerables de Tecnologías de Información con un Enfoque de Auditoría Basado en Riesgos en el Ecuador*. 2011.

Young, Ernst &. *Cambios en el panorama de los riesgos de TI*. 2010.

ANEXO 1

CUADRO COMPARATIVO DE INSTITUCIONES MICROFINANCIERA DE LA REGIÓN LAMBAYEQUE

	MICROFINANCIERA 1	MICROFINANCIERA 2	MICROFINANCIERA 3
ANTIGÜEDAD	18 años de creación.	22 años como entidad regulada.	16 años de creación como entidad regulada.
CREACIÓN DE LA EMPRESA	Nació como Edpyme en el año 1999 y desde el 2010 se convirtió en financiera.	Empezó sus operaciones en el año 1995 como Caja Rural Cruz de Chalpón y en el año 2006 cambió su nombre.	Inició en el año 1992 como un Programa de Financiamiento y Asistencia Técnica para las Pequeñas y Micro Empresas.
GRUPO ECONÓMICO	Forma parte del Grupo EFE, operando como brazo financiero de sus empresas vinculadas: Conecta Retail S.A. (Tiendas Efe y Curacao) y Motocorp S.A.	Forma parte del Grupo Perales Huancaruna.	Forma parte del Grupo Diviso.
OFICINAS	Sede Principal en la ciudad de Chiclayo, Lambayeque.		
	Dispone de una red de 193 oficinas a nivel nacional.	Cuenta con 6 agencias y 3 oficinas informativas en los departamentos de Libertad, Lambayeque, Cajamarca y San Martín.	Cuenta con 20 agencias y 7 oficinas informativas en los departamentos de Piura, Lambayeque, Amazonas, Cajamarca, La Libertad y San Martín.
MISIÓN	La organización tiene como objetivo que las operaciones de créditos sean desarrolladas con eficacia, creciendo en colocaciones, con eficiencia, definiendo el apetito y tolerancia al riesgo crediticio, y contando con una adecuada gestión de cobranzas.	Los clientes se sienten satisfechos, con el acceso y uso a servicios financieros mediante sus dispositivos digitales y, con una cálida atención al acompañarlos en su desarrollo.	Brindar soluciones financieras que atiendan necesidades de Emprendedores y Microempresarios, con una alta vocación de servicio.
VISIÓN	Empresa líder en brindar servicios y facilidades financieras a sectores de menores ingresos de la población con reducido sustento documentario.	Facilitar el progreso económico y social de la población emergente, sin exclusión alguna, con servicios financieros innovadores y responsables, que respondan a sus necesidades y sueños.	Ser la Institución reconocida por su Agilidad, Flexibilidad y Excelencia en el servicio hacia sus clientes.

	MICROFINANCIERA 1	MICROFINANCIERA 2	MICROFINANCIERA 3
VALORES	· Meritocracia. · Profesionalismo. · Desarrollo. · Compromiso Corporativo. · Ética.	· Honestidad. · Equidad. · Respeto. · Responsabilidad y Compromiso. · Adaptación al Cambio.	· Honestidad. · Cooperación. · Lealtad. · Respeto. · Servicio.
ORIENTACIÓN DEL SERVICIO	Especialista en colocaciones de crédito de consumo principalmente originadas en las empresas vinculadas.	Especialista en prestar servicios de crédito a distintos nichos de la población: Micro Empresa, Pequeña Empresa y Mediana Empresa y Créditos de Consumo.	Especialista en prestar servicios financieros a zonas rurales.
ENTIDADES REGULADORAS	· Superintendencia de Banca, Seguros y AFP (SBS). · Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). · Banco Central de Reserva (BCR). · Superintendencia Nacional de Fiscalización Laboral (SUNAFIL). · Superintendencia Nacional de Administración Tributaria (SUNAT).		
GESTIÓN DE RIESGOS	Cuenta con la Gerencia de Riesgos y Gerencia de Auditoría. Cuenta con un manual para la gestión de riesgos.	Cuenta con Gerencia de Riesgos y Unidad de Auditoría Interna. Cuenta con un manual para la gestión de riesgos con el objetivo que tengan una intervención activa en los procesos críticos de la entidad, especialmente en el seguimiento de las actividades del equipo de negocios y operaciones.	Cuenta con Unidad de Riesgos y Unidad de Auditoría Interna. Cuenta con un manual que alinean un conjunto de principios y establecen un marco para la Gestión y Supervisión eficaces de los Riesgos.
ÁREA DE SISTEMAS	Depende de la Gerencia General conformado por más de 50 personas organizados en las siguientes áreas: Desarrollo, Infraestructura y Comunicaciones, Producción, Control de Proyectos, Inteligencia de Negocios, Seguridad.	Depende de la Gerencia General conformado 7 personas organizados en dos sub áreas: Desarrollo y Producción y Soporte	Depende de la Gerencia General conformado por 10 personas distribuidos en dos áreas: Soporte y Desarrollo.

ANEXO 2

ENCUESTA DE DIAGNÓSTICO DE LA GESTIÓN DE RIESGOS DE TI

NOMBRE: _____ **FECHA:**_____
EMPRESA: _____
CARGO: _____

Marque con una "X" la respuesta que considere más adecuada y si lo cree conveniente escriba un comentario explicativo

	ESTABLECIMIENTO DEL CONTEXTO	SI	PARCIAL	NO	COMENTARIO
1	¿Se ha establecido un marco de referencia para la gestión de riesgos de TI?				
2	¿Se gestionan los riesgos de acuerdo a los objetivos, parámetros internos y externo de la organización?				
3	¿Se encuentran determinados los objetivos, el alcance y las actividades de la gestión de riesgos de TI?				
4	¿La gestión de riesgos de TI cuenta con los recursos, responsabilidades y autoridades necesarios?				
5	¿La organización tiene definidos los criterios para evaluar la importancia de los riesgos de TI?				
6	¿La organización cuenta con algún manual o procedimiento para la gestión de riesgos de TI?				

	EVALUACIÓN DEL RIESGO	SI	PARCIAL	NO	COMENTARIO
7	¿La organización tiene identificados y registrados los activos principales?				
8	¿Se tienen claramente identificados los riesgos a los que están expuestos los activos en base a las vulnerabilidades y amenazas?				
9	¿La organización tiene identificados las fuentes del riesgo, las áreas de impacto, los eventos, y sus causas y consecuencias potenciales?				
9.7	¿Se encuentra disponible la información pertinente y actualizada para la identificación de riesgos de TI?				
11	¿Se involucra al personal con el conocimiento apropiado para la identificación del riesgo?				
12	¿Se considera la interdependencia y el origen de los riesgos de TI?				
13	¿Se priorizan los riesgos según su impacto en los objetivos organizacionales?				

	TRATAMIENTO DEL RIESGO	SI	PARCIAL	NO	COMENTARIO
14	¿La organización cuenta con un proceso de tratamiento de riesgos de TI?				
15	¿Los tratamientos de riesgos se ejecutan teniendo en cuenta un orden de prioridad según el análisis del riesgo?				
16	¿Los planes de tratamiento de riesgos se encuentran integrados con los procesos de gestión de la organización?				
17	¿Los encargados de la toma de decisiones y partes interesadas evidencian conocer la naturaleza y extensión del riesgo residual después del tratamiento del riesgo de TI?				

	MONITOREO Y REVISIÓN	SI	PARCIAL	NO	COMENTARIO
18	¿La organización cuenta con un proceso de monitoreo para la gestión de riesgos?				
19	¿El monitoreo se realiza de manera periódica?				
20	¿Se encuentran claramente definidas las responsabilidades del monitoreo y la revisión?				

	COMUNICACIÓN Y CONSULTA	SI	PARCIAL	NO	COMENTARIO
21	¿Se tienen desarrollados planes de comunicación de riesgo, sus causas y sus consecuencias, y las medidas para tratarlo?				
22	¿Son eficaces la comunicación y las consultas externas e internas garantizando la toma de decisiones de los responsables de la gestión de riesgos de TI?				
23	¿Se toman en cuenta los puntos de vistas y las percepciones de las partes involucradas en la toma de decisiones relacionadas a la gestión de riesgos de TI?				

	ANALISIS DE IMPACTO DE NEGOCIO (BIA)	SI	PARCIAL	NO	COMENTARIO
24	¿La institución cuenta con un BIA?				
25	¿El compromiso de liderazgo de la organización para la continuidad del negocio es visible?				
26	¿Existe una política de continuidad del negocio que sea apropiada, mantenida, comunicada y documentada?				
27	¿La política se encuentra disponible para los empleados y todas las partes interesadas?				
28	¿Se tiene un análisis de amenazas y oportunidades que pueden impactar en la continuidad del negocio?				
29	¿Está toda la organización consciente de la importancia de la política de continuidad del negocio?				
30	¿Existe un proceso formal y documentado para la comprensión de la organización a través de un BIA?				

ANEXO 3

COMPARACIÓN DE METODOLOGÍAS, ESTÁNDARES Y MARCOS DE TRABAJO DE GESTIÓN DE RIESGOS

ISO 31000	ISO 27005	OCTAVE	MAGERIT	COBIT 5 para Riesgos
PROCESO 1: Establecer el contexto - Establecer el contexto externo. - Establecer el contexto interno. - Establecer el contexto del proceso de gestión de riesgos. - Definir criterios de riesgo.	**PROCESO 1: Establecimiento del contexto** - Definir alcance y límites. - Definir criterios de: evaluación del Riesgo, probabilidad, impacto y aceptación del riesgo.	**PROCESO 1: Visión organizativa** - Definir activos. - Definir amenazas. - Definir vulnerabilidades - Definir requerimientos de seguridad.	**PROCESO 1: Método de análisis de riesgos** - Determinación del alcance del proyecto. - Planificación del proyecto. - Lanzamiento del proyecto.	- Incluye prácticas de gestión para comprender el contexto interno y externo. - El dominio gobierno del riesgo asegura que el enfoque adoptado de gestión de riesgos es adecuado para la situación de la empresa. - Ofrece una guía a las empresas para desarrollar sus criterios específicos de riesgos. - El modelo de catalizadores incluye prácticas de gestión para establecer los criterios del riesgo.
PROCESO 2: Identificar riesgo - Identificar las fuentes de riesgo, zonas de impactos, los acontecimientos y sus causas y sus posibles consecuencia.	**PROCESO 2: Valoración del riesgo** - Identificación del riesgo. - Estimación del riesgo. - Evaluación del riesgo.		**PROCESO 2: Análisis de riesgos** - Caracterización de los activos. - Caracterización de las amenazas. - Caracterización de las salvaguardas. - Estimación del estado de riesgo.	- Incluye prácticas de gestión para identificar los riesgos asociados con los productos y servicios clave de la organización que dependen de TI. - Incluye técnicas específicas para identificar escenarios basados en un actor, tipo de amenaza, evento, recursos/ activos y una dimensión de tiempo.
PROCESO 3: Analizar Riesgos - Identificar causas y las		**PROCESO 2: Visión tecnológica** - Definir componentes		El análisis del riesgo es el proceso que estima la frecuencia y El impacto de los escenarios de

ISO 31000	ISO 27005	OCTAVE	MAGERIT	COBIT 5 para Riesgos
fuentes del riesgo, su impacto positivo y negativo y la probabilidad de ocurrencia.		claves. - Vulnerabilidades técnicas.		riesgo.
PROCESO 4: Evaluar riesgos - Comparación del nivel de riesgo identificado durante el proceso de análisis con criterios de riesgo establecidos.		**PROCESO 3: Estrategia y Desarrollo del plan** - Identificar riesgos. -Identificar estrategias de protección. - Establecer planes de mitigación.		Aborda esta fase del proceso en forma intrínseca.
PROCESO 5: Tratar riesgos - Seleccionar de opciones de tratamiento del riesgo. - Preparar y ejecutar planes de tratamiento del riesgo.	**PROCESO 3: Tratamiento del riesgo** - Reducir el riesgo. - Evitar el riesgo. - Transferir el riesgo. **PROCESO 4: Aceptación del riesgo** - Convivir con el riesgo.		**PROCESO 3: Gestión de riesgos** - Identificación de planes de seguridad. - Planificación de los proyectos de seguridad. - Ejecución del plan.	- Incluye una guía sobre las opciones comunes de respuesta y cómo se aplican en un contexto de TI. - Define respuestas específicas al riesgo para abordar diferentes tratamientos del riesgo. - Utiliza desarrollo de escenarios para la identificación de riesgos.
PROCESO 6: Monitorear y revisar - Seguir y revisar los controles.	**PROCESO 5: Monitoreo y revisión del riesgo** - Monitoreo y Revisión del Proceso. - Monitoreo y Revisión de Los Factores de Riesgo.			Incluye metas y métricas que pueden ser utilizadas para medir el desempeño, y un modelo de madurez para establecer una hoja de ruta para mejorar el proceso de gestión de riesgos.
PROCESO 7: Comunicar y consultar - Planificar la comunicación interna y externa.	**PROCESO 6: Comunicación del riesgo** - Entendimiento de la probabilidad y las consecuencias de los riesgos.			El habilitador “Información” incluye información específica a ser comunicada entre las partes interesadas.

ANEXO 4

EJEMPLOS DE VULNERABILIDADES Y AMENAZAS (ISO 27005)

TIPO	EJEMPLO DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Hardware	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Brechas de mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico	Destrucción de equipamiento o medios
	Susceptible a humedad, polvo	Polvo, corrosión
	Sensibilidad a radiación electromagnética	Radiación electromagnética
	Falta de un eficiente control de cambios en la configuración	Error en el uso
	Susceptible a variaciones de voltaje	Pérdida de alimentación eléctrica
	Susceptible a variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento desprotegido	Robo de medios o documentos
	Falta de cuidado en el desecho / disposición de equipos	Robo de medios o documentos
	Falta de control de copiado	Robo de medios o documentos
Software	Falta o insuficiencia de pruebas de software	Abuso de privilegios
	Fallas conocidas en el software	Abuso de privilegios
	Falta de controles para el cierre de sesión en terminales desatendidas	Abuso de privilegios
	Desecho o reutilización de medios de almacenamiento sin un borrado apropiado	Abuso de privilegios
	Falta de pistas de auditoría	Abuso de privilegios
	Incorrecta asignación de privilegios de acceso	Abuso de privilegios
	Software ampliamente distribuido	Corrupción de datos
	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	Corrupción de datos
	Interfaz de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Parametrización incorrecta	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autenticación	Suplantación de identidad
	Tablas de claves secretas (passwords) desprotegidos	Suplantación de identidad
	Pobre gestión de claves secretas (passwords)	Suplantación de identidad
	Servicios innecesarios habilitados	Procesamiento ilegal de datos
	Software inmaduro	Mal funcionamiento de software
	Especificaciones poco claras o incompletas para desarrolladores	Mal funcionamiento de software
	Falta de un control de cambios efectivo	Mal funcionamiento de software
	Descarga y uso de software no controlados	Manipulación de software
	Falta de copias de respaldo	Manipulación de software
	Falta de protección física del edificio, puertas y ventanas	Robo de medios o documentos
	Falta de control para la producción de reportes gerenciales	Uso no autorizado de equipamiento

TIPO	EJEMPLO DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Red	Falta de prueba del envió o la recepción de mensajes	Negociación de acciones
	Líneas de comunicación sin protección	Escucha subrepticia
	Trafico sensible sin protección	Escucha subrepticia
	Conexión deficiente de los cables	Falla de equipo de telecomunicaciones
	Punto único de fallas	Falla de equipo de telecomunicaciones
	Falta de identificación y autenticación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia de personal	Brechas en la disponibilidad del personal
	Procedimientos inadecuados de reclutamiento	Destrucción de equipo o medios
	Entrenamiento de seguridad insuficiente	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de concientización en seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo del personal de limpieza no supervisado	Robo de medios o documentos
	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería	Uso no autorizado de equipo
Centro de cómputo	Uso inadecuado o descuidado de controles de acceso físico a edificios y cuartos	Destrucción de equipo o medios
	Localización en un área susceptible a inundaciones	Inundación
	Alimentación de energía eléctrica inestable	Pérdida de provisión de energía eléctrica
	Falta de protección física del edificio, puertas y ventanas	Robo de equipo
Organización	Falta de procedimientos formales para el registro y des-registro de usuarios	Abuso de privilegios
	Falta de procedimientos formales para la revisión de derechos de acceso (supervisión)	Abuso de privilegios
	Falta o insuficiencia de provisiones (relativas a seguridad) en contratos con clientes y/o terceras partes	Abuso de privilegios
	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	Abuso de privilegios
	Falta de auditorías regulares (supervisión)	Abuso de privilegios
	Falta de procedimientos para la identificación y evaluación de riesgos	Abuso de privilegios
	Falta de reportes de falla registrados en bitácoras de administrador y operador	Abuso de privilegios

TIPO	EJEMPLO DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Mantenimiento de servicios inadecuado	Brechas en el mantenimiento de sistemas de información
	Falta o insuficiencia de acuerdos de niveles de servicio	Brechas en el mantenimiento de sistemas de información
	Falta de procedimientos de control de cambios	Brechas en el mantenimiento de sistemas de información
	Falta de procedimientos formales para el control de documentos del Sistema de Gestión de Seguridad de la Información	Corrupción de datos
	Falta de procedimientos formales para la supervisión de registros del Sistema de Gestión de Seguridad de la Información	Corrupción de datos
	Falta de procesos formales para la autorización de información públicamente disponible	Datos de fuentes no confiables
	Falta de asignación apropiada de responsabilidades de seguridad de la información	Denegación de acciones
	Falta de planes de continuidad	Falla de equipos
	Falta de políticas de uso de correo electrónico	Error en el uso
	Falta de procedimientos para la introducción se software en sistemas operativos	Error en el uso
	Falta de registros en las bitácoras de administrador y operador	Error en el uso
	Falta de procedimientos para el manejo de información clasificada	Error en el uso
	Falta de descripciones de puesto que indiquen responsabilidades de seguridad de la información	Error en el uso
	Falta o insuficiencia de provisiones (respecto a la seguridad de la información) en contratos con empleados	Procesamiento ilegal de datos
	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Robo de equipo
	Falta de control de activos fuera de las instalaciones	Robo de equipo
	Falta o insuficiencia de políticas de “escritorio limpio” y “pantalla limpia”	Robo de medios o documentos
	Falta de autorización de instalaciones de procesamiento de información	Robo de medios o documentos
	Falta de mecanismos de monitoreo establecidos para violaciones a la seguridad	Robo de medios o documentos
	Falta de revisiones de la gerencia en forma regular	Uso no autorizado de equipo
	Falta de procedimientos para el reporte de debilidades de seguridad	Uso no autorizado de equipo
	Falta de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual	Uso de software falsificado o copiado

ANEXO 5

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.
Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : _____
FORMACIÓN ACADÉMICA : _____
AREAS DE EXPERIENCIA PROFESIONAL: _____
TIEMPO DE EXPERIENCIA : _____
CARGO ACTUAL : _____
INSTITUCIÓN : _____

Objetivo de la investigación : Contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque mediante el desarrollo de un modelo de gestión de riesgos de TI.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para las microfinacieras de la región Lambayeque.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1 No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1 No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1 No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN DEL
MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Establecimiento del Contexto	Definir el contexto externo					
	Definir el contexto interno					
Análisis de impacto de negocio (BIA)	Identificar procesos					
	Evaluar el impacto del negocio					
	Establecer periodos de tiempo					
	Establecer el nivel de criticidad de los procesos					
Identificación del riesgo	Identificar activos					
	Valorar activos					
	Identificar amenazas y vulnerabilidades					

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Análisis del riesgo	Definir criterios del riesgo					
	Estimar el riesgo					
Evaluación del riesgo	Priorizar riesgos					
	Valorar riesgos					
Tratamiento del riesgo	Seleccionar estrategias de tratamiento					
	Proponer planes de acción					
Monitoreo y revisión						
Comunicación y consulta						

Comentario Final:

_____
_____
_____
_____
_____

ANEXO 6

RESULTADO DE VALIDACIÓN DE EXPERTOS DEL MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	EXPERTO 1				EXPERTO 2				EXPERTO 3			
		SU	CO	RE	CL	SU	CO	RE	CL	SU	CO	RE	CL
Establecimiento del Contexto	Definir el contexto externo	4	4	4	3	3	3	4	4	3	3	3	3
	Definir el contexto interno	3	4	3	3	3	3	3	4	3	3	3	3
Análisis de impacto de negocio (BIA)	Identificar procesos	4	4	3	4	3	4	4	4	3	4	4	3
	Evaluar el impacto del negocio	3	3	3	4	2	1	3	4	3	4	4	3
	Establecer periodos de tiempo	4	3	3	4	3	4	4	4	3	4	4	3
	Establecer el nivel de criticidad de los procesos	4	3	3	3	3	4	4	4	3	4	4	3
Identificación del riesgo	Identificar activos	4	4	4	4	3	4	4	4	3	4	4	3
	Valorar activos	4	4	3	4	3	3	4	4	3	4	4	3
	Identificar amenazas y vulnerabilidades	4	4	3	4	3	3	4	4	3	4	4	3
Análisis del riesgo	Definir criterios del riesgo	4	4	3	4	4	4	4	4	3	4	4	3
	Estimar el riesgo	4	4	3	4	4	4	4	4	3	4	4	3
Evaluación del riesgo	Priorizar riesgos	3	4	3	4	2	3	3	4	3	4	4	3
	Valorar riesgos	3	4	3	4	3	3	3	4	3	4	4	3
Tratamiento del riesgo	Seleccionar estrategias de tratamiento	3	4	3	4	4	3	3	4	3	4	4	3
	Proponer planes de acción	3	4	3	4	3	3	3	4	3	4	4	3
Monitoreo y revisión		2	3	2	4	2	3	4	3	3	4	4	3
Comunicación y consulta		2	3	3	4	3	4	4	4	3	4	4	3

Experto 1 – Revisión 1

Ernesto Karlo Celi Arevalo <eceli@unprg.edu.pe> 6 ene.
para mí

Remito las observaciones a su propuesta, las cuales básicamente se resumen en dos grandes aspectos:
1. Su modelo es muy genérico y no está todavía personalizado para entidades financieras
2. Su modelo es solo para evaluar riesgos de TI, pero su modelo propuesto abarca todos los tipos de riesgos que potencialmente pueden ocurrir en una entidad financiera

Sin embargo, el modelo de manera general está bien planteado y ordenado. Realicen los ajustes necesarios y luego me lo vuelven a remitir para evaluarlo.

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS	: Ernesto Karlo Celi Arévalo
FORMACIÓN ACADÉMICA	: Ingeniero de Computación y Sistemas
AREAS DE EXPERIENCIA PROFESIONAL: Auditoría y Gestión de Riesgos de TI	
TIEMPO DE EXPERIENCIA	: 22 años
CARGO ACTUAL	: Director de Escuela Profesional Ingeniería de Sistemas
INSTITUCIÓN	: Universidad Nacional Pedro Ruiz Gallo

Objetivo de la investigación	: Contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque mediante el desarrollo de un modelo de gestión de riesgos de TI.
Objetivo del juicio de expertos	: Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad del modelo propuesto para las microfinacieras de la región Lambayeque.

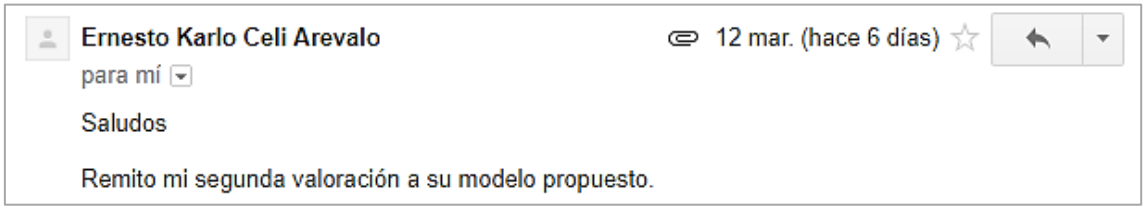
De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CUESTIONARIO PARA VALIDACIÓN DEL

MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Establecimiento del Contexto	Definir el contexto externo	2	4	2	3	El modelo no está personalizado y contextualizado para entidades microfinancieras por lo que todavía falta mejorar la suficiencia y coherencia
	Definir el contexto interno	2	4	2	3	El modelo no está personalizado y contextualizado para entidades microfinancieras por lo que todavía falta mejorar la suficiencia y coherencia
Análisis de impacto de negocio (BIA)	Identificar procesos	2	3	2	4	El modelo no está personalizado y contextualizado para entidades microfinancieras por lo que todavía falta mejorar la suficiencia y coherencia
	Evaluar el impacto del negocio	2	3	3	4	El modelo no está personalizado y contextualizado para entidades microfinancieras por lo que todavía falta mejorar la suficiencia y coherencia
	Establecer periodos de tiempo	4	3	2	4	El modelo propuesto es genérico para todo tipo de riesgos, cuando la investigación es para los riesgos de TI. No se observa esta diferencia
	Establecer el nivel de criticidad de los procesos	4	3	2	3	El modelo propuesto es genérico para todo tipo de riesgos, cuando la investigación es para los riesgos de TI. No se observa esta diferencia
Identificación del riesgo	Identificar activos	4	4	2	4	El modelo propuesto es genérico para todo tipo de riesgos, cuando la investigación es para los riesgos de TI. No se observa esta diferencia
	Valorar activos	4	4	3	4	
	Identificar amenazas y vulnerabilidades	4	4	3	4	
Análisis del riesgo	Definir criterios del riesgo	4	4	3	4	
	Estimar el riesgo	4	4	3	4	
Evaluación del riesgo	Priorizar riesgos	3	4	3	4	
	Valorar riesgos	3	4	3	4	
Tratamiento del riesgo	Seleccionar estrategias de tratamiento	3	4	3	4	
	Proponer planes de acción	3	4	3	4	
Monitoreo y revisión		2	3	2	4	
Comunicación y consulta		2	3	3	4	

Experto 1 – Revisión 2



Ernesto Karlo Celi Arevalo 12 mar. (hace 6 días)

para mí

Saludos

Remito mi segunda valoración a su modelo propuesto.

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTION DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGION LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS	: Ernesto Karlo Celi Arévalo
FORMACION ACADEMICA	: Ingeniero en Computación y Sistemas Magister en Ciencias con mención en Informática y Sistemas Doctor en Administración
AREAS DE EXPERIENCIA PROFESIONAL:	Auditoría y Gestión de Riesgos de TI
TIEMPO DE EXPERIENCIA	: más de 22 años
CARGO ACTUAL	: Director de la Escuela Profesional de Ingeniería de Sistemas y Coordinador Académico de la Maestría en Ingeniería de Sistemas de la UNPRG
INSTITUCION	: Universidad Nacional Pedro Ruiz Gallo
Objetivo de la investigación	: Contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque mediante el desarrollo de un modelo de gestión de riesgos de TI.
Objetivo del juicio de expertos	: Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad del modelo propuesto para las microfinancieras de la región Lambayeque.

CUESTIONARIO PARA VALIDACIÓN DEL

MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Establecimiento del Contexto	Definir el contexto externo	4	4	4	3	
	Definir el contexto interno	3	4	3	3	El detalle de la gestion de riesgos de TI en las instituciones que tomaron como casos de estudio no describen con claridad el cumplimiento de las exigencias de la SBS
Análisis de impacto de negocio (BIA)	Identificar procesos	4	4	3	4	El análisis BIA se realiza por proceso y en cada análisis se identifican los activos, su criticidad, el RTO y el RPO.
	Evaluar el impacto del negocio	3	3	3	4	
	Establecer periodos de tiempo	4	3	3	4	
	Establecer el nivel de criticidad de los procesos	4	3	3	3	
Identificación del riesgo	Identificar activos	4	4	4	4	
	Valorar activos	4	4	3	4	
	Identificar amenazas y vulnerabilidades	4	4	3	4	
Análisis del riesgo	Definir criterios del riesgo	4	4	3	4	
	Estimar el riesgo	4	4	3	4	
Evaluación del riesgo	Priorizar riesgos	3	4	3	4	
	Valorar riesgos	3	4	3	4	
Tratamiento del riesgo	Seleccionar estrategias de tratamiento	3	4	3	4	
	Proponer planes de acción	3	4	3	4	Falta incluir indicadores de riesgos (KPR)
Monitoreo y revisión		2	3	2	4	
Comunicación y consulta		2	3	3	4	

Experto 2 – Revisión 1

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

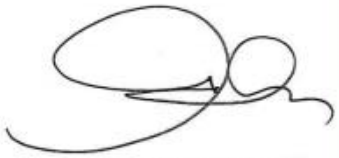
Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : Iman Espinoza Ricardo David
FORMACIÓN ACADÉMICA : Ing. Sistemas y Computación
AREAS DE EXPERIENCIA PROFESIONAL: Tecnologías de Información
TIEMPO DE EXPERIENCIA : 8 años de experiencia
CARGO ACTUAL : Docente Tiempo Completo Fac. Ingeniería
INSTITUCIÓN : USAT

Objetivo de la investigación : Contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque mediante el desarrollo de un modelo de gestión de riesgos de TI.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para las microfinacieras de la región Lambayeque.



RICARDO DAVID IMAN ESPINOZA
INGENIERO DE SISTEMAS
Reg. C.I.P. 149364

CUESTIONARIO PARA VALIDACIÓN DEL
MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Establecimiento del Contexto	Definir el contexto externo	3	3	4	4	Establecer formato de identificación de Est. Contexto Externo
	Definir el contexto interno	2	2	3	4	Establecer formato de identificar Contexto Interno
Análisis de impacto de negocio (BIA)	Identificar procesos	3	4	4	4	Se podría cuantificar los ítems / formular agrega mas procesos
	Evaluar el impacto del negocio	2	1	3	4	Cuantificar los ítems
	Establecer periodos de tiempo	2	1	3	4	evidenciar el número de horas (fuente)
falta c	Establecer el nivel de criticidad de los procesos	2	1	3	4	Evidenciar el número de días (fuente)
Identificación del riesgo	Identificar activos	3	4	4	4	Permitir agregar mas activos
	Valorar activos	2	1	3	4	Cuantificar los ítems
	Identificar amenazas y vulnerabilidades	~~2~~ 3	3	4	4	~~identificar fuente de anexo 04~~ Agregar sobre el contexto financiero

Análisis del riesgo	Definir criterios del riesgo	4	4	4	4	identificar fuente
	Estimar el riesgo	4	4	4	4	Agregar ejemplos en la plantilla.
Evaluación del riesgo	Priorizar riesgos	1	2	3	4	Agregar detalle de como llegar al mapa de calor
	Valorar riesgos	3	3	3	4	agregar ejemplos en la plantilla.
Tratamiento del riesgo	Seleccionar estrategias de tratamiento	4	3	3	4	Establecer formato para la Estrategia
	Proponer planes de acción	1	2	3	4	Dar mas detalle. Pag. 94
Monitoreo y revisión						
Comunicación y consulta						

Experto 2 – Revisión 2

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : Ricardo David Irman Espinoza
FORMACIÓN ACADÉMICA : Ing. Sistemas y Computación
AREAS DE EXPERIENCIA PROFESIONAL: Tecnologías de Información
TIEMPO DE EXPERIENCIA : 8 años de experiencia
CARGO ACTUAL : Docente Tiempo Completo Fac Ingeniería.
INSTITUCIÓN : USAT

Objetivo de la investigación : Contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque mediante el desarrollo de un modelo de gestión de riesgos de TI.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para las microfinacieras de la región Lambayeque.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

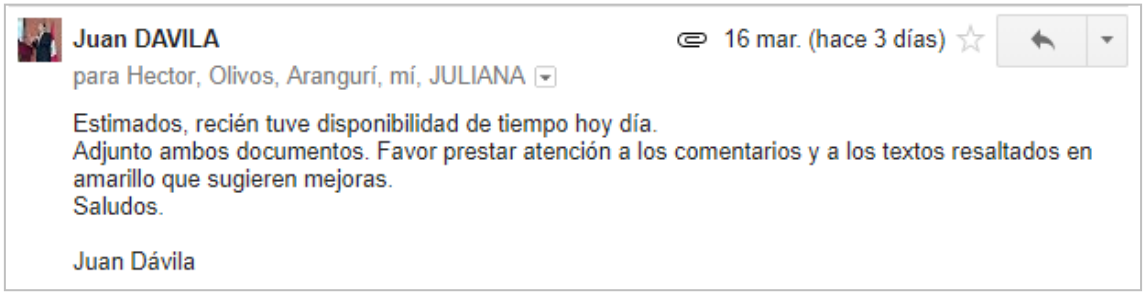
CUESTIONARIO PARA VALIDACIÓN DEL

MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Establecimiento del Contexto	Definir el contexto externo	3	3	4	4	
	Definir el contexto interno	3	3	3	4	
Análisis de impacto de negocio (BIA)	Identificar procesos	3	4	4	4	
	Evaluar el impacto del negocio	2	1	3	4	determinar: poco regular grande etc
	Establecer periodos de tiempo	3	4	4	4	
	Establecer el nivel de criticidad de los procesos	3	4	4	4	
Identificación del riesgo	Identificar activos	3	4	4	4	
	Valorar activos	3	3	4	4	
	Identificar amenazas y vulnerabilidades	3	3	4	4	agregar sobre el contexto financiero
Análisis del riesgo	Definir criterios del riesgo	4	4	4	4	identificar fuente.
	Estimar el riesgo	4	4	4	4	
Evaluación del riesgo	Priorizar riesgos	2	3	3	4	dar mejor detalle explicar el procedimiento
	Valorar riesgos	3	3	3	4	
Tratamiento del riesgo	Seleccionar estrategias de tratamiento	4	3	3	4	incluir contexto financiero.
	Proponer planes de acción	3	3	3	4	
Monitoreo y revisión		2	3	4	3	
Comunicación y consulta		3	4	4	4	

Comentario Final: La propuesta del modelo define estructura básica y fundamental para la gestión de Riesgos de TI, establece plantillas y criterios donde con el contexto es recomendable proponer amenazas predifinidas sobre el contexto financiero.

Experto 3



Juan DAVILA 16 mar. (hace 3 días)

para Hector, Olivos, Arangurí, mí, JULIANA

Estimados, recién tuve disponibilidad de tiempo hoy día.
Adjunto ambos documentos. Favor prestar atención a los comentarios y a los textos resaltados en amarillo que sugieren mejoras.
Saludos.

Juan Dávila

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA CONTINUIDAD DEL NEGOCIO DE LAS MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : JUAN DÀVILA RAMÌREZ
FORMACIÓN ACADÉMICA : INGENIERO INDUSTRIAL
AREAS DE EXPERIENCIA PROFESIONAL: GOBIERNO, RIESGOS, SEGURIDAD DE INFORMACIÓN Y AUDITORÍA DE TI
TIEMPO DE EXPERIENCIA : 24 AÑOS
CARGO ACTUAL : DIRECTOR
INSTITUCIÒN : PROTIVITI

Objetivo de la investigación : Contribuir a la continuidad del negocio de las microfinancieras de la región Lambayeque mediante el desarrollo de un modelo de gestión de riesgos de TI.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para las microfinacieras de la región Lambayeque.

CUESTIONARIO PARA VALIDACIÓN DEL
MODELO DE GESTIÓN DE RIESGOS DE TI PARA MICROFINANCIERAS DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Establecimiento del Contexto	Definir el contexto externo	3	3	3	3	
	Definir el contexto interno	3	3	3	3	
Análisis de impacto de negocio (BIA)	Identificar procesos	3	4	4	3	
	Evaluar el impacto del negocio	3	4	4	3	
	Establecer periodos de tiempo	3	4	4	3	
	Establecer el nivel de criticidad de los procesos	3	4	4	3	
Identificación del riesgo	Identificar activos	3	4	4	3	
	Valorar activos	3	4	4	3	
	Identificar amenazas y vulnerabilidades	3	4	4	3	
Análisis del riesgo	Definir criterios del riesgo	3	4	4	3	
	Estimar el riesgo	3	4	4	3	
Evaluación del riesgo	Priorizar riesgos	3	4	4	3	
	Valorar riesgos	3	4	4	3	
Tratamiento del riesgo	Seleccionar estrategias de tratamiento	3	4	4	3	
	Proponer planes de acción	3	4	4	3	
Monitoreo y revisión		3	4	4	3	
Comunicación y consulta		3	4	4	3	

ANEXO 7

APLICACIÓN DEL MÉTODO PROPUESTO

A continuación se muestra un ejemplo de la aplicación del método propuesto a la microfinanciera 3 a la cual la mencionaremos solo como microfinanciera

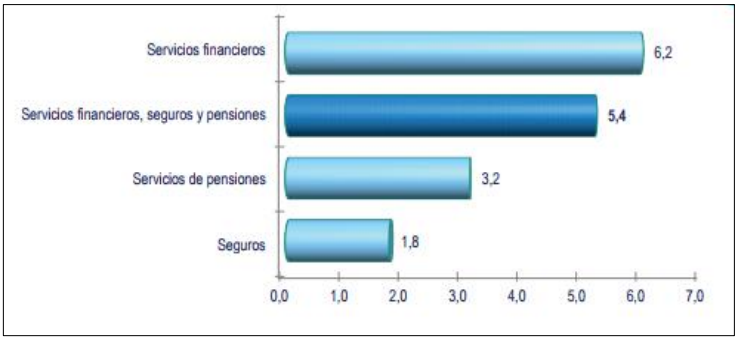
Fase I: Establecimiento del contexto

Actividad 1: Definir el contexto externo

El análisis del contexto externo contempla los siguientes aspectos:

DEFINICIÓN DE CONTEXTO EXTERNO	**CÓDIGO: P001**
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	
ASPECTO	**DESCRIPCIÓN**
Sociocultural	Además de la educación y la concientización, uno de los principales obstáculos en el Perú es el elevado costo de las transferencias y transacciones inherentes ligadas a los productos, sobre todo en zonas remotas. No obstante las iniciativas de educación financiera, el fomento del usuario de la tecnología y la reducción de costos de transacciones está permitiendo a los bancos dar a conocer sus productos. Con la legislación del dinero electrónico, que permite a los operadores móviles y otras entidades afines emitir y transferir dinero electrónico, se estima que se generará la apertura de una gama más extensa de productos.
Económico	En el Perú la orientación del crédito está muy concentrada en el sector de los ingresos medios y altos. Pero existe un sector del 60% de la población que no acceden al crédito bancario, por lo tanto hace falta una mayor democratización del crédito con los sectores de menor ingresos lo cual conlleva a que los entes reguladores desarrollen políticas más inclusivas q ayuden a la democracia del crédito. El valor agregado bruto de la actividad servicios financieros, seguros y pensiones registró un crecimiento de 5,4% respecto al año anterior, destacando el incremento de la actividad servicios financieros (6,2%).

DEFINICIÓN DE CONTEXTO EXTERNO	CÓDIGO: P001
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	

ASPECTO	DESCRIPCIÓN
	El crecimiento de la actividad servicios financieros fue impulsado por el aumento de los créditos otorgados por la banca múltiple y cajas municipales de ahorro y crédito; y de la actividad seguros principalmente por el aumento de las primas de seguros de vida y las primas de accidentes y enfermedades.  Fuente: (INEI 2016)
Competitivo	La competencia que existe en la región Lambayeque es directa, ya que con el crecimiento de la región, cada vez son más las instituciones financieras que tienen presencia en la región Lambayeque. Actualmente son 14 microfinancieras que operan en la región, pero solo 2 son las que trabajan con empresas retail que se dedican a otorgar créditos de consumo al sector socioeconómico C y D.
Tecnológico	El aspecto tecnológico ha cobrado bastante importancia en el sector microfinanciero, el avance de la tecnología permite a estas empresas diversificar los productos que ofrecen y brindar mucha mejor atención a los clientes.
Reglamentario	El sector microfinanciero está fuertemente regulado por las siguientes instituciones: • Superintendencia de Banca, Seguros y AFP (SBS). • Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). • Banco Central de Reserva (BCR). • Superintendencia Nacional de Fiscalización Laboral (SUNAFIL). • Superintendencia Nacional de Administración

DEFINICIÓN DE CONTEXTO EXTERNO	CÓDIGO: P001
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	

ASPECTO	DESCRIPCIÓN
	Tributaria (SUNAT).
Proveedores	Se cuentan con proveedores principalmente para los siguientes servicios: • Telefonía IP • Internet • Póliza de Seguros • Seguridad • Central de Riesgos

Actividad 2: Definir el contexto interno

El análisis del contexto interno contempla los siguientes aspectos:

DEFINICIÓN DE CONTEXTO INTERNO	CÓDIGO: P002
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	

ASPECTO	DESCRIPCIÓN
Estructura organizacional	En la microfinanciera, la estructura organizacional es formal y jerárquica, cuenta con una junta general de accionistas el cual es el órgano supremo de la sociedad quienes deciden por mayoría los asuntos propios de su competencia. El Directorio es el órgano colegiado elegido por la Junta General o Junta Especial, tiene las facultades de gestión y representación legal necesarias para la administración de la sociedad dentro de su objetivo. Es conformada por seis miembros, que son elegidos por periodos de tres años, teniendo la posibilidad de ser reelegidos indefinidamente.
Cultura organizacional	La cultura organizacional está orientada al servicio al cliente y esto se refleja en su misión, visión y valores las cuales se detallan a continuación:

DEFINICIÓN DE CONTEXTO INTERNO	CÓDIGO: P002
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	
ASPECTO	**DESCRIPCIÓN**
	Misión La organización tiene como objetivo que las operaciones de créditos sean desarrolladas con eficacia, creciendo en colocaciones, con eficiencia, definiendo el apetito y tolerancia al riesgo crediticio, y contando con una adecuada gestión de cobranzas. **Visión** Empresa líder en brindar servicios y facilidades financieras a sectores de menores ingresos de la población con reducido sustento documentario. **Valores** • Respeto a la persona: Presumir la honestidad y lealtad de los clientes y sociedad en general, salvo que bajo fundadas razones haya sospecha o la posibilidad de existencia de alguna actuación ilegítima. • Lealtad: Cumplimiento de las normas de fidelidad y honor actuando con verdad y consecuencia con los principios que rigen la actividad empresarial, frente a quienes puedan hacer uso incorrecto de la microfinanciera. • Honestidad: Actuar con honestidad, veracidad, transparencia, elevado sentido de responsabilidad y profesionalismo, debiendo dichos actos responder a la confianza que la sociedad y los clientes depositan en la la microfinanciera. • Equidad, Justicia y respeto mutuo: En las relaciones con los clientes, con los competidores y con las múltiples instancias con las cuales interactúan, distinguiendo la legítima actuación de las que no lo son.

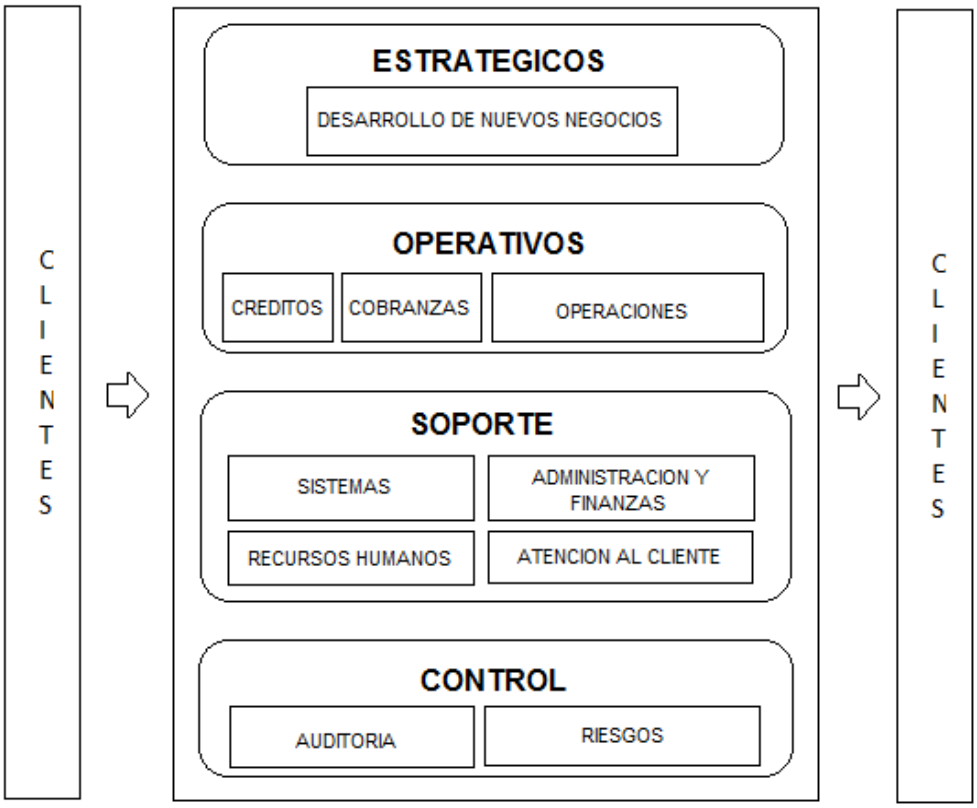
DEFINICIÓN DE CONTEXTO INTERNO	CÓDIGO: P002
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	

ASPECTO	DESCRIPCIÓN
	• Confidencialidad: La microfinanciera y los trabajadores deberán proteger la información que les ha sido confiada y las que conozcan como consecuencia de las operaciones que realizan los clientes, así como la de la Institución de acuerdo a lo establecido en el Manual de Procedimientos de Prevención contra el Lavado de Activos, sin que ello signifique encubrimiento o colaboración con personas deshonestas, estén o no protegidas por el Secreto Bancario. • Integridad en el uso de los recursos: Utilizar los recursos en bien y provecho de las actividades lícitas y permitidas por la legislación vigente y el Estatuto de la microfinanciera.
Objetivos organizacionales	Debido a la naturaleza del negocio, la microfinanciera ha determinado los siguientes objetivos estratégicos: • Incremento de las colocaciones y desembolsos anuales. • Crecimiento de la empresa con la diversificación de negocios (otros canales). • Fidelizar al cliente. • Optimizar los procesos operativos, administrativos y de gestión de riesgos, así como contar con una mejor infraestructura y con un equipamiento moderno. • Consolidar estrategias que faciliten la captación de nuevos clientes y la toma de decisiones acertadas.
Sistemas de información	La microfinanciera cuenta con diversos sistemas de información que automatizan, la gestión administrativa, gestión financiera, retail e inteligencia de negocio. Éstos se detallan en el ítem de identificación de activos.

Fase II: Análisis de impacto de negocio

Actividad 1: Identificar procesos

IDENTIFICACIÓN DE PROCESOS	CÓDIGO: P003
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	



Según el mapa de procesos de la microfinanciera se han identificados los siguientes macroprocesos principales en base lo conversado con el personal de apoyo de dicha organización:

- Macroproceso de otorgamiento de crédito (CRÉDITOS)
- Macroproceso de captaciones. (OPERACIONES)
- Macroproceso de cobranza. (COBRANZAS)

- Macroproceso de atención al cliente. (ATENCIÓN AL USUARIO)

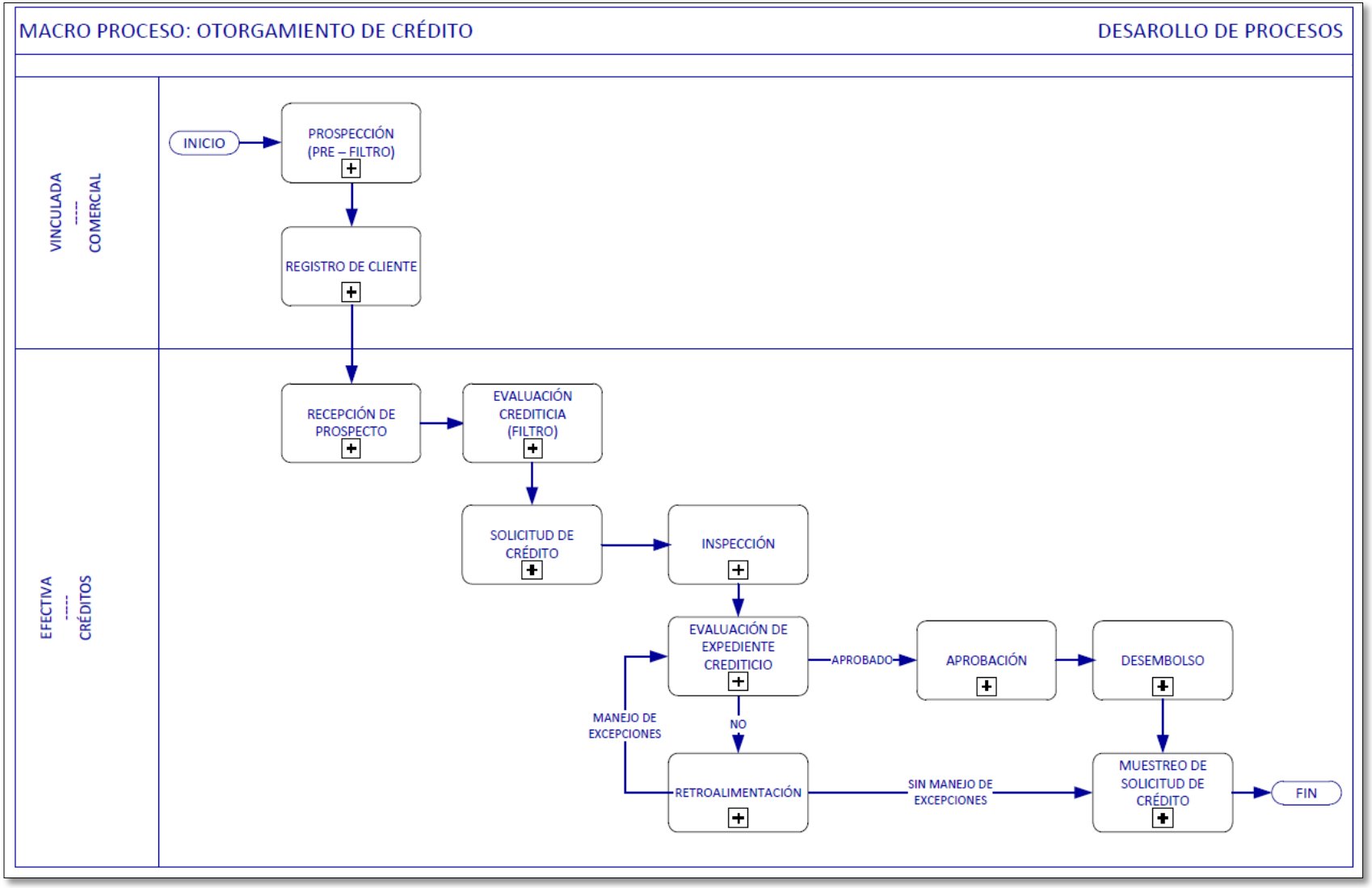
A continuación detalla cada macroproceso de otorgamiento de crédito y cobranza y además se identifican sus procesos:

a. Macroproceso de otorgamiento de crédito (MPO_OTC)

Permite evaluar al cliente de manera formal ante centrales de riesgos y define las características necesarias para que el cliente pueda acceder a los productos que ofrece la financiera.

Se identifican los siguientes procesos:

- Proceso de prospección (PO_P).
- Proceso de registro del cliente (PO_RC).
- Proceso de evaluación crediticia (PO_EC).
- Proceso de solicitud de crédito (PO_SC).
- Proceso de inspección (PO_I).
- Proceso de evaluación (PO_EV)
- Proceso de aprobación (PO_AP).
- Proceso de desembolso (PO_DES).


MACRO PROCESO: OTORGAMIENTO DE CRÉDITO
DESAROLLO DE PROCESOS
VINCULADA

COMERCIAL
EFECTIVA

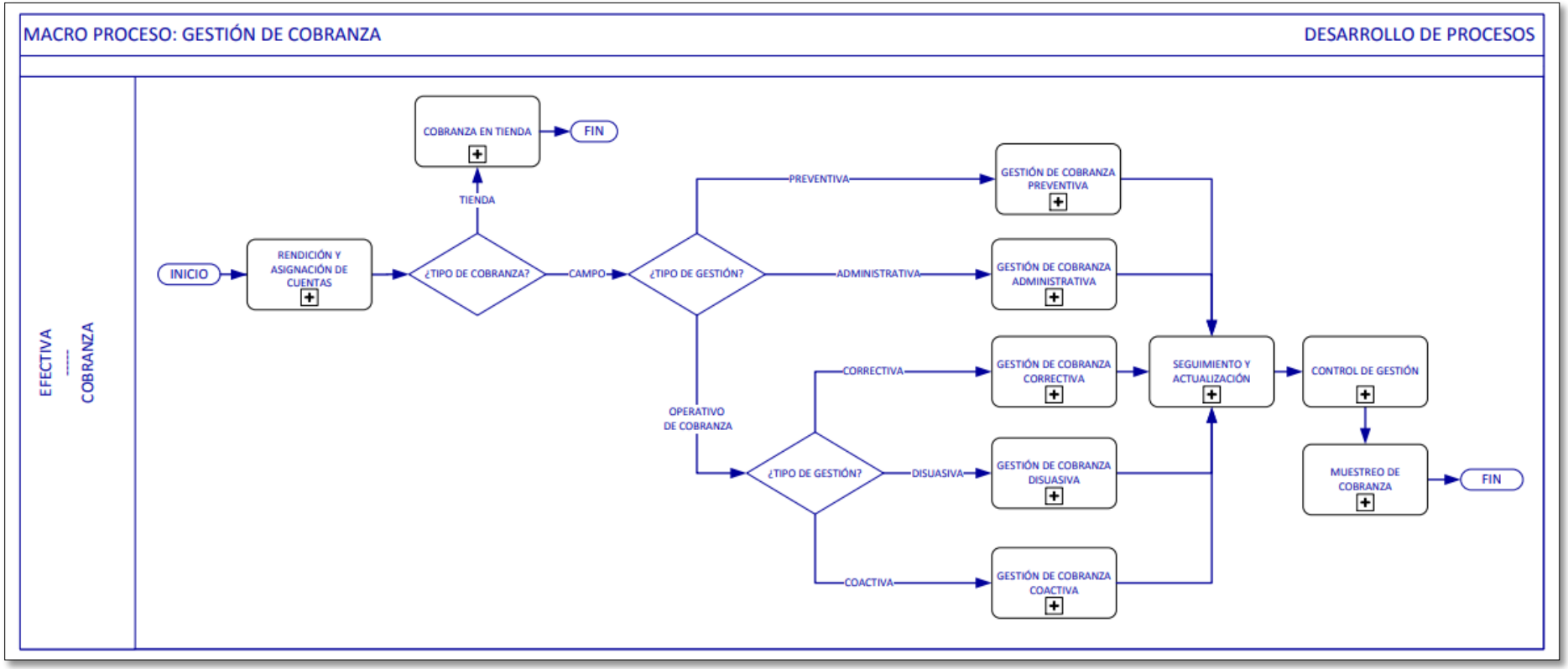
CRÉDITOS
INICIO
PROSPECCIÓN (PRE – FILTRO)
REGISTRO DE CLIENTE
RECEPCIÓN DE PROSPECTO
EVALUACIÓN CREDITICIA (FILTRO)
SOLICITUD DE CRÉDITO
INSPECCIÓN
EVALUACIÓN DE EXPEDIENTE CREDITICIO
APROBADO
APROBACIÓN
DESEMBOLSO
MANEJO DE EXCEPCIONES
NO
RETROALIMENTACIÓN
SIN MANEJO DE EXCEPCIONES
MUESTREO DE SOLICITUD DE CRÉDITO
FIN

b. Macroproceso de cobranza (MPO_COB)

Acciones desarrolladas por el personal de cobranza para requerir el pago de una deuda atrasada a clientes de la financiera. Puede hacerse vía telefónica, presencial, vía carta u otros canales permitidos por la legislación vigente.

Los procesos que comprenden este macroproceso son los siguientes:

- Proceso de Cobranza en Tienda (PO_CT).
- Proceso Gestión Cobranza Preventiva (PO_GCP).
- Proceso Gestión de Cobranza Administrativa (PO_GCA).
- Proceso Gestión de Cobranza Correctiva (PO_CO).
- Proceso Gestión de Cobranza Disuasiva (PO_GCD).
- Proceso Gestión de Cobranza Coactiva (PO_GCC).


MACRO PROCESO: GESTIÓN DE COBRANZA
DESARROLLO DE PROCESOS
EFECTIVA
COBRANZA
INICIO
RENDICIÓN Y ASIGNACIÓN DE CUENTAS
¿TIPO DE COBRANZA?
TIENDA
COBRANZA EN TIENDA
FIN
CAMPO
¿TIPO DE GESTIÓN?
PREVENTIVA
GESTIÓN DE COBRANZA PREVENTIVA
ADMINISTRATIVA
GESTIÓN DE COBRANZA ADMINISTRATIVA
OPERATIVO DE COBRANZA
¿TIPO DE GESTIÓN?
CORRECTIVA
GESTIÓN DE COBRANZA CORRECTIVA
DISUASIVA
GESTIÓN DE COBRANZA DISUASIVA
COACTIVA
GESTIÓN DE COBRANZA COACTIVA
SEGUIMIENTO Y ACTUALIZACIÓN
CONTROL DE GESTIÓN
MUESTREO DE COBRANZA
FIN

c. Macroproceso de captaciones (MPO_CAP).

Consiste en la recepción de depósitos en cuentas corrientes bancarias, cuentas de ahorro o depósitos a plazo fijo a cambio de lo cual se le paga una tasa de interés al cliente.

- Proceso de apertura de cuenta (MPO_APCB).
- Proceso de administración de cuenta (MPO_ADCB).
- Proceso de cierre de cuenta (MPO_CCB).

d. Macroproceso de atención al cliente (MPO_ATC).

Permite atender reclamos, sugerencias o inquietudes de los clientes sobre algún producto o servicio brindado por la microfinanciera.

Actividad 2: Evaluar el impacto del negocio

A partir de los macroprocesos y procesos identificados, se establece un valor para el impacto financiero, regulatorio y reputacional.

IMPACTO EN EL NEGOCIO DE LOS PROCESOS				**CÓDIGO: P004**		
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
UNIDAD DE NECOGIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**IMPACTO**		
				F	**R**	**RE**
AREA DE CREDITOS Y RIESGOS	MPO_OTC	PO_P	Módulo de gestión de Otorgamiento de crédito	3	1	1
		PO_RC		3	1	1
		PO_EC		3	1	1
		PO_SC		3	1	1
		PO_I		3	1	1
		PO_EV		3	1	1
		PO_AP		4	3	3
		PO_DES		5	3	3
AREA DE OPERACIONES	MPO_CAP	PO_APCB	Módulo de gestión de captaciones	3	5	3
		PO_ADCB		3	4	3
		PO_CCB		1	4	1
AREA DE COBRANZAS	MPO_COB	PO_CT	Módulo de gestión de cobranza	5	3	2
		PO_GCP		3	4	2
		PO_GCA		3	4	2
		PO_CO		3	4	2
		PO_GCD		3	4	2
		PO_GCC		3	4	2

IMPACTO EN EL NEGOCIO DE LOS PROCESOS				CÓDIGO: P004		
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
UNIDAD DE NECOGIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**IMPACTO**		
				F	**R**	**RE**
AREA DE ATENCION AL USUARIO	MPO_ATC	PO_ATC	Sistema de postventa	2	3	4

Se observa que el proceso de otorgamiento de crédito tiene un alto impacto financiero en los procesos de aprobación y desembolso dado que estas actividades son las que generan ingresos a la microfinanciera por lo tanto el área de TI debe prestar el soporte de calidad correspondiente para prevalecer la continuidad del proceso.

En el proceso de captaciones se observa que tiene un alto impacto regulatorio dado que los servicios prestados en este proceso afecta considerablemente el capital del cliente.

También se observa que el proceso de cobranza tiene un alto impacto regulatorio por las amonestaciones que podrían afectar a la microfinanciera por cobros indebidos, además tiene a su vez un impacto financiero dado que el incumplimiento de pagos de los clientes afecta directamente los ingresos de la financiera.

El proceso de atención al cliente; es considerado un proceso menor pero no menos importante que los demás dado que presenta un impacto reputacional debido a que involucra el trato y servicio al cliente.

Actividad 3: Establecer periodos de tiempo

A partir de los macroprocesos y procesos identificados, se establece un valor para el RTO, RPO, MDT.

ESTABLECIMIENTO DE TIEMPOS POR PROCESOS						CÓDIGO: P005
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
UNIDAD DE NECOGIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**RTO**	**RPO**	**MTPD**
AREA DE CREDITOS Y RIESGOS	MPO_OTC	PO_P	Módulo de gestión de colocaciones	3	24h	4
		PO_RC		3	24h	4
		PO_EC		3	24h	4
		PO_SC		3	24h	3
		PO_I		3	24h	3
		PO_EV		3	24h	3
		PO_AP		2	24h	2
		PO_DES		2	24h	2
AREA DE OPERACIONES	MPO_CAP	PO_APCB	Módulo de gestión de captaciones	3	24h	2
		PO_ADCB		3	24h	3
		PO_CCB		2	24h	4
AREA DE COBRANZAS	MPO_COB	PO_CT	Módulo de gestión de cobranza	2	24h	2
		PO_GCP		3	24h	4
		PO_GCA		3	24h	4
		PO_CO		3	24h	4
		PO_GCD		3	24h	4
		PO_GCC		3	24h	4
AREA DE ATENCION AL USUARIO	MPO_ATC	PO_ATC	Sistema de postventa	4	24h	4

Para todos los procesos se observa que el periodo máximo tolerable de pérdida de datos es de 24 horas dado que según indagaciones con el personal de operaciones del área de TI en la financiera, el proceso de backup se realiza diariamente.

Con respecto al proceso de otorgamiento crediticio el tiempo establecido por la empresa para reanudar el proceso (RTO) es de 4 horas para los procesos de alto impacto financiera. Y el tiempo que podría afectar la viabilidad de la microfinanciera (MDT) es pasada las 24 horas.

Actividad 4: Establecer el nivel de criticidad de los procesos

Por cada proceso se establece su nivel de criticidad.

CRITICIDAD DE LOS PROCESOS					CÓDIGO: P006
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.					
UNIDAD DE NECOGIO	**MACRO PROCESO**	**PROCESOS**	**DEPENDENCIA SERVICIOS TI**	**MTPD**	**ESCALA**
ÁREA DE CRÉDITOS Y RIESGOS	MPO_OTC	PO_P	Módulo de gestión de colocaciones	4	Sensible
		PO_RC		4	Sensible
		PO_EC		4	Sensible
		PO_SC		3	Vital
		PO_I		3	Vital
		PO_EV		3	Vital
		PO_AP		2	Crítico
		PO_DES		2	Crítico
ÁREA DE OPERACIONES	MPO_CAP	PO_APCB	Módulo de gestión de captaciones	2	Crítico
		PO_ADCB		3	Vital
		PO_CCB		4	Sensible
ÁREA DE COBRANZAS	MPO_COB	PO_CT	Módulo de gestión de cobranza	2	Crítico
		PO_GCP		4	Sensible
		PO_GCA		4	Sensible
		PO_CO		4	Sensible
		PO_GCD		4	Sensible
		PO_GCC		4	Sensible
ÁREA DE ATENCIÓN AL USUARIO	MPO_ATC	PO_ATC	Sistema de postventa	4	Sensible

Se observa que los procesos críticos identificados son los procesos de aprobación, desembolso, apertura de cuentas y cobranza de tienda, puesto que su desarrollo depende a gran escala del correcto funcionamiento del sistema.

Fase III: Identificación del riesgo

Actividad 1: Identificar activos

De los macro procesos anteriormente mencionados, todos ellos se manejan a través del sistema financiero integral y por tanto comparten los mismos recursos. A continuación se describe cada uno de ellos.

IDENTIFICACIÓN DE ACTIVOS					CÓDIGO: P007
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.					
N°	**CÓDIGO**	**NOMBRE**	**DESCRIPCION**	**RESPONSABLE**	**TIPO**
1	HW_PC	Computadora de escritorio	Equipo de cómputo usado por los trabajadores de la organización	Área de sistemas	Hardware
2	HW_IMP	Impresora	Equipo de cómputo usado por los trabajadores de la organización	Área de sistemas	Hardware
3	HW_CE	Cableado Ethernet	Suministro para las comunicaciones en red	Área de sistemas	Hardware
4	HW_FW	Firewall	Equipo de cómputo para evitar el ingreso de virus	Área de sistemas	Hardware
5	HW_UPS	UPS	Activo usado para cortes de energía	Área de sistemas	Hardware
6	HW_BDP	Servidor BD Primario	Activo que almacena data de producción	Área de sistemas	Hardware
7	HW_BDS	Servidor BD Secundario	Activo que almacena data de producción	Área de sistemas	Hardware
8	HW_CO	Servidor Correo	Activo que almacena toda la mensajería de la organización	Área de sistemas	Hardware
9	SW_LMW	Licencia de software	Licencias para utilizar un software adquirido a terceros	Área de sistemas	Software
10	SW_PWI	Página Web de la Institución	Sitio web de la organización	Área de RRHH	Software
11	SW_II	Intranet de la Institución	Sito web para capacitación al personal	Área de RRHH	Software
12	SW_SOC	Sistema Operativo	Software usado para el funcionamiento de PCs, laptops y servidores	Área de sistemas	Software

IDENTIFICACIÓN DE ACTIVOS					CÓDIGO: P007
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.					
N°	**CÓDIGO**	**NOMBRE**	**DESCRIPCION**	**RESPONSABLE**	**TIPO**
13	SW_SFI	Sistema Financiero Integral	Software core de la organización	Gerencia General	Software
14	SW_SAP	Sistema SAP	ERP administrativo	Gerencia de administración	Software
15	S_CE	Servicio de correo electrónico	servicio de mensajería	Área de sistemas	Servicio
16	S_EQX	Servicio a Equifax	Servicio de acceso a central de riesgos	Gerencia de riesgos	Servicio
17	S_IT	Servicio de internet	Servicio de acceso a internet	Área de sistemas	Servicio
18	P_ORIG	Proceso de originación	Módulo del Sistema financiero integral	Gerencia de riesgos	Proceso
19	P_DESEM	Proceso de desembolso	Módulo del sistema financiero integral	Gerencia de créditos	Proceso
20	P_CD	Proceso de cierre diario	Módulo del sistema financiero integral	Gerencia de sistemas	Proceso
21	P_CM	Proceso de cierre mensual	Módulo del sistema financiero integral	Gerencia de sistemas	Proceso
22	P_CC	Proceso de cobranza	Módulo del sistema financiero integral	Gerencia de cobranzas	Proceso
23	MEDIA_BBD	Backup de base de datos	Copia de seguridad de la base de datos	Área de sistemas	Soporte de información

Actividad 2: Valorar activos

Por cada activo identificado, se evalúan los criterios de confidencialidad, integridad, disponibilidad y cumplimiento normativo.

VALORIZACIÓN DE ACTIVOS							CÓDIGO: P008
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
N°	**ACTIVO**	**CRITERIOS**				**TOTAL**	**NIVEL DE CRITICIDAD**
		C	**I**	**D**	**N**		
1	Computadora de escritorio	3	2	3	1	3	Medio
2	Impresora	3	1	2	1	3	Medio

VALORIZACIÓN DE ACTIVOS	CÓDIGO: P008

Elaborado por: Analista de riesgo operacional.

Revisado por: Gerente de riesgos.

Aprobado por: Comité de riesgos.

N°	ACTIVO	CRITERIOS				TOTAL	NIVEL DE CRITICIDAD
		C	I	D	N		
3	Cableado Ethernet	3	2	3	2	3	Medio
4	Firewall	3	2	3	3	3	Medio
5	UPS	4	3	4	4	4	Alto
6	Servidor BD Primario	5	5	5	5	5	Muy alto
7	Servidor BD Secundario	3	4	2	2	2	Alto
8	Servidor Correo	3	2	3	2	3	Medio
9	Licencia de software	4	4	4	4	4	Alto
10	Página Web de la Institución	2	3	3	2	3	Medio
11	Intranet de la Institución	3	2	3	2	3	Medio
12	Sistema Operativo	4	3	3	2	4	Alto
13	Sistema Financiero Integral	4	5	5	4	5	Muy alto
14	Sistema SAP	4	5	5	3	5	Muy alto
15	Servicio de correo electrónico	3	3	5	3	5	Muy alto
16	Servicio a Equifax	4	4	5	4	5	Muy alto
17	Servicio de internet	2	5	5	3	5	Muy alto
18	Proceso de originación	5	5	5	4	5	Muy alto
19	Proceso de desembolso	5	5	5	4	5	Muy alto
20	Proceso de cierre diario	5	5	5	4	5	Muy alto
21	Proceso de cierre mensual	5	5	5	4	5	Muy alto
22	Proceso de cobranza	5	5	5	4	5	Muy alto
23	Backup de base de datos	5	5	5	4	5	Muy alto

Actividad 3: Identificar amenazas y vulnerabilidades

Por cada activo se identifican las amenazas que explotan sus vulnerabilidades.

IDENTIFICACIÓN DE AMENAZAS			CÓDIGO: P009
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.			
Nº	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**
1	Computadora de escritorio	Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico
2	Impresora	Robo de medios o documentos	Almacenamiento desprotegido
3	Cableado Ethernet	Escucha subrepticia	Líneas de comunicación sin protección
		Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.
4	Firewall	Polvo, corrosión	Susceptible a humedad, polvo
		Falla de equipo de telecomunicaciones	Punto único de fallas
		Espionaje remoto	Arquitectura insegura de la red
5	UPS	Falla de equipos	Falta de planes de continuidad
		Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico
		Sensibilidad a radiación electromagnética	Radiación electromagnética
6	Servidor BD Primario	Manipulación con software	Falta de copias de respaldo
		Robo de medios o documentos	Falta de autorización de instalaciones de procesamiento de información
7	Servidor BD Secundario	Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información
		Error en el uso	Falta de un eficiente control de cambios en la configuración
8	Servidor Correo	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación
		Falla de equipo de telecomunicaciones	Punto único de fallas
		Espionaje remoto	Transferencia de contraseñas autorizadas

IDENTIFICACIÓN DE AMENAZAS			CÓDIGO: P009
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.			
Nº	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**
9	Licencias de software	Uso de software falsificado o copiado	Falta de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual
		Corrupción de datos	Software ampliamente distribuido
		Abuso de privilegios	Falta de controles para el cierre de sesión en terminales desatendidas
10	Página Web de la Institución	Mal funcionamiento de software	Falta de control eficaz del cambio
11	Intranet de la Institución	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios
12	Sistema Operativo	Error en el uso	Falta de procedimientos para la introducción se software en sistemas operativos
		Suplantación de identidad	Pobre gestión de claves secretas (passwords)
		Manipulación de software	Descarga y uso de software no controlados
13	Sistema Financiero Integral	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios
		Abuso de privilegios	Falta de pistas de auditoría
		Error en el uso	Falta de documentación
		Abuso de privilegios	Falta de procedimientos formales para la revisión de derechos de acceso (supervisión)
14	Sistema SAP	Error en el uso	Uso incorrecto de software y hardware
		Error en el uso	Interfaz de usuario complicada
15	Servicio a Equifax	Brechas en el mantenimiento de sistemas de información	Mantenimiento de servicios inadecuado
		Error en el uso	Parametrización incorrecta
		Procesamiento ilegal de datos	Servicios innecesarios habilitados

IDENTIFICACIÓN DE AMENAZAS			CÓDIGO: P009
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.			
Nº	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**
16	Servicio de correo electrónico	Error en el uso	Falta de políticas de uso de correo electrónico
		Negociación de acciones	Falta de prueba del envió o la recepción de mensajes
17	Servicio de internet	Uso no autorizado de equipo	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería
		Conexiones de red pública sin protección	Uso no autorizado del equipo
18	Proceso de originación	Mal funcionamiento de software	Especificaciones poco claras o incompletas para desarrolladores
		Saturación del sistema de información	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)
19	Proceso de desembolso	Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia de acuerdos de niveles de servicio
		Error en el uso	Falta de procedimientos para la introducción se software en sistemas operativos
		Abuso de privilegios	Falta o insuficiencia de pruebas de software
20	Proceso de cierre diario	Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador
		Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información
21	Proceso de cierre mensual	Procesamiento ilegal de los datos	Falta de mecanismos de monitoreo
		Uso no autorizado de equipo	Falta de revisiones de la gerencia en forma regular
22	Proceso de cobranza	Abuso de los derechos	Defectos bien conocidos en el software
23	Backup de base de datos	Destrucción de equipo o medios	Procedimientos inadecuados de reclutamiento
		Manipulación de software	Falta de copias de respaldo

Fase IV: Análisis del riesgo

Actividad 1: Definir criterios del riesgo

Se establecen los criterios para evaluar los riesgos.

VALOR	PROBABILIDAD [P]	DESCRIPCIÓN
1	Raro	Puede ocurrir en circunstancias excepcionales 1 vez cada 5 años.
2	Improbable	Se podría presentar una vez cada 5 años.
3	Posible	Se podría presentar una vez al año.
4	Poco probable	Se podría presentar una vez cada mes.
5	Casi seguro	Se podría presentar varias veces en el mes.

VALOR	IMPACTO [I]	DESCRIPCIÓN
1	Insignificante	Tiene un efecto nulo o muy pequeño en las operaciones
2	Menor	Afecta parcialmente las operaciones.
3	Moderado	Operativamente es sostenible, pero dificulta o retrasa las operaciones.
4	Mayor	Paraliza la atención de servicios críticos a clientes, debido a la caída significativa de las operaciones.
5	Catastrófico	Paraliza todas las operaciones de la entidad.

RANGO	NIVEL DE RIESGO	DESCRIPCIÓN
1 – 5	1	Bajo
6 – 10	2	Medio
11 – 15	3	Alto
16 – 25	4	Extremo

Actividad 2: Estimar el riesgo

Por cada amenaza se establece la probabilidad e impacto.

ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**P**	**I**	**PXI**	**RIESGO**	
							CÓDIGO	**NIVEL**
1	Computadora de escritorio	Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	4	1	4	R1	Bajo
2	Impresora	Robo de medios o documentos	Almacenamiento desprotegido	4	1	4	R2	Bajo
3	Cableado Ethernet	Escucha subrepticia	Líneas de comunicación sin protección	3	4	12	R3	Alto
		Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.	4	4	16	R4	Extremo
4	Firewall	Polvo, corrosión	Susceptible a humedad, polvo	2	4	8	R5	Medio
		Falla de equipo de telecomunicaciones	Punto único de fallas	1	4	4	R6	Bajo
		Espionaje remoto	Arquitectura insegura de la red	2	4	8	R7	Medio
5	UPS	Falla de equipos	Falta de planes de continuidad	3	4	12	R8	Alto
		Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	1	3	3	R9	Bajo
		Sensibilidad a radiación	Radiación electromagnética	1	2	2	R10	Bajo

ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**P**	**I**	**PXI**	**RIESGO**	
							CÓDIGO	**NIVEL**
		electromagnética						
6	Servidor BD Primario	Manipulación con software	Falta de copias de respaldo	4	5	20	R11	Extremo
		Robo de medios o documentos	Falta de autorización de instalaciones de procesamiento de información	5	5	25	R12	Extremo
7	Servidor BD Secundario	Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	5	5	25	R13	Extremo
		Error en el uso	Falta de un eficiente control de cambios en la configuración	3	4	12	R14	Alto
8	Servidor Correo	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación	2	3	6	R15	Medio
		Falla de equipo de telecomunicaciones	Punto único de fallas	3	5	15	R16	Alto
		Espionaje remoto	Transferencia de contraseñas autorizadas	2	5	10	R17	Medio

ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**P**	**I**	**PXI**	**RIESGO**	
							CÓDIGO	**NIVEL**
9	Licencias de software	Uso de software falsificado o copiado	Falta de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual	3	3	9	R18	Medio
		Corrupción de datos	Software ampliamente distribuido	2	4	8	R19	Medio
		Abuso de privilegios	Falta de controles para el cierre de sesión en terminales desatendidas	2	4	8	R20	Medio
10	Página Web de la Institución	Mal funcionamiento de software	Falta de control eficaz del cambio	3	1	3	R21	Bajo
11	Intranet de la Institución	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	4	1	4	R22	Bajo
12	Sistema Operativo	Error en el uso	Falta de procedimientos para la introducción se software en sistemas operativos	3	3	9	R23	Medio
		Suplantación de identidad	Pobre gestión de claves secretas (passwords)	3	5	15	R24	Alto

ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**P**	**I**	**PXI**	**RIESGO**	
							CÓDIGO	**NIVEL**
		Manipulación de software	Descarga y uso de software no controlados	3	3	9	R25	Medio
13	Sistema Financiero Integral	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	5	5	25	R26	Extremo
		Abuso de privilegios	Falta de pistas de auditoría	4	1	4	R27	Bajo
		Error en el uso	Falta de documentación	4	3	12	R28	Alto
		Abuso de privilegios	Falta de procedimientos formales para la revisión de derechos de acceso (supervisión)	5	3	15	R29	Alto
14	Sistema SAP	Error en el uso	Uso incorrecto de software y hardware	5	3	15	R30	Alto
		Error en el uso	Interfaz de usuario complicada	5	3	15	R31	Alto

ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**P**	**I**	**PXI**	**RIESGO**	
							CÓDIGO	**NIVEL**
15	Servicio a Equifax	Brechas en el mantenimiento de sistemas de información	Mantenimiento de servicios inadecuado	5	5	25	R32	Extremo
		Error en el uso	Parametrización incorrecta	3	4	12	R33	Alto
		Procesamiento ilegal de datos	Servicios innecesarios habilitados	2	3	6	R34	Medio
16	Servicio de correo electrónico	Error en el uso	Falta de políticas de uso de correo electrónico	5	3	15	R35	Alto
		Negociación de acciones	Falta de prueba del envió o la recepción de mensajes	3	2	6	R36	Medio
17	Servicio de internet	Uso no autorizado de equipo	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería	5	5	25	R37	Extremo
		Conexiones de red pública sin protección	Uso no autorizado del equipo	5	4	20	R38	Extremo
18	Proceso de originación	Mal funcionamiento de software	Especificaciones poco claras o incompletas para desarrolladores	5	5	25	R39	Extremo

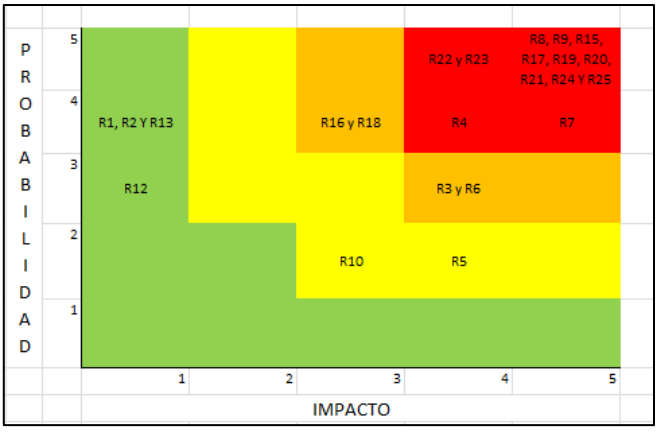
ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**P**	**I**	**PXI**	**RIESGO**	
							CÓDIGO	**NIVEL**
		Saturación del sistema de información	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	3	5	15	R40	Alto
19	Proceso de desembolso	Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia de acuerdos de niveles de servicio	5	5	25	R41	Extremo
		Error en el uso	Falta de procedimientos para la introducción se software en sistemas operativos	1	4	4	R42	Bajo
		Abuso de privilegios	Falta o insuficiencia de pruebas de software	3	3	9	R43	Medio
20	Proceso de cierre diario	Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador	5	4	20	R44	Extremo

ANÁLISIS DE RIESGOS								CÓDIGO: P010
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.								
N°	ACTIVO	AMENAZA	VULNERABILIDAD	P	I	PXI	RIESGO	
							CÓDIGO	NIVEL
		Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	5	4	20	R45	Extremo
21	Proceso de cierre mensual	Procesamiento ilegal de los datos	Falta de mecanismos de monitoreo	5	4	20	R46	Extremo
		Uso no autorizado de equipo	Falta de revisiones de la gerencia en forma regular	5	3	15	R47	Alto
22	Proceso de cobranza	Abuso de los derechos	Defectos bien conocidos en el software	5	5	25	R48	Extremo
23	Backup de base de datos	Destrucción de equipo o medios	Procedimientos inadecuados de reclutamiento	5	5	25	R49	Extremo
		Manipulación de software	Falta de copias de respaldo	5	3	15	R50	Alto

Fase V: Evaluación del riesgo

Actividad 1: Priorizar riesgos

En base a lo trabajado en el apartado anterior se obtiene el mapa de calor tabulando en la matriz según la probabilidad e impacto.



Actividad 2: Valorar riesgos

Se establece la tolerancia y apetito de riesgo y partir de ello se valoriza al riesgo.

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R1	Bajo	Computadora de escritorio	Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	4	3	6	Tolerable	La amenaza no representa un impacto fuerte en la continuidad del negocio porque se puede habilitar una nueva computadora con el backup de la información que contenía la computadora averiada
R2	Bajo	Impresora	Robo de medios o documentos	Almacenamiento desprotegido	4	6	12	Aceptable	La información confidencial no se imprime en impresoras compartidas, por tanto, si hay robo de documentos no será de información sensible

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R3	Alto	Cableado Ethernet	Escucha subrepticia	Líneas de comunicación sin protección	12	6	8	Intolerable	El filtro de información de clientes y cuentas a través de la red es crítico porque expone la información confidencial de clientes
R4	Extremo		Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.	16	8	12	Intolerable	La conectividad de las agencias se considera crítica ya que afecta el proceso de cobranza y desembolso
R5	Medio	Firewall	Polvo, corrosión	Susceptible a humedad, polvo	8	6	12	Tolerable	La falla del equipo expone a la empresa a ataques informáticos pero existen otros medios de seguridad para contrarrestarlos
R6	Bajo		Falla de equipo de telecomunicaciones	Punto único de fallas	4	6	8	Aceptable	
R7	Medio		Espionaje remoto	Arquitectura insegura de la red	8	8	12	Tolerable	
R8	Alto	UPS	Falla de equipos	Falta de planes de continuidad	12	6	8	Intolerable	La falla de equipos UPS generan deficiencias en los planes de continuidad de negocio

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R9	Bajo		Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	3	4	6	Aceptable	Los UPS están conservados en buen estado y por falta de presupuesto es difícil su renovación
R10	Bajo		Sensibilidad a radiación electromagnética	Radiación electromagnética	2	4	6	Aceptable	
R11	Extremo	Servidor BD Primario	Manipulación con software	Falta de copias de respaldo	20	6	8	Intolerable	La información guardada en el servidor primario debe tener backups periódicos que no presenten fallas al ser restaurados
R12	Extremo		Robo de medios o documentos	Falta de autorización de instalaciones de procesamiento de información	25	12	16	Intolerable	En el servidor secundario se guarda información sensible, el robo de información causaría un gran impacto
R13	Extremo	Servidor BD Secundario	Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	25	9	16	Intolerable	El servidor secundario no debe ser accedido por personas no autorizadas por poseer información sensible

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R14	Alto		Error en el uso	Falta de un eficiente control de cambios en la configuración	12	8	10	Intolerable	El servidor secundario debe tener un control adecuado de las configuraciones
R15	Medio	Servidor Correo	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación	6	8	9	Aceptable	Se realizan backups periódicos por lo que la información puede ser recuperada y la seguridad física está bien resguardada
R16	Alto		Falla de equipo de telecomunicaciones	Punto único de fallas	15	6	10	Intolerable	La falla del servidor de correo por determinado tiempo no paraliza las actividades de la empresa pero si resulta importante para los procesos de soporte.
R17	Medio		Espionaje remoto	Transferencia de contraseñas autorizadas	10	4	6	Intolerable	La confidencialidad de la información se ve violada sino se gestionan las contraseñas de acceso

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R18	Medio	Licencias de software	Uso de software falsificado o copiado	Falta de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual	9	6	12	Tolerable	Algunas computadoras pueden tener programas no licenciados como apoyo a sus tareas pero los principales sistemas si están licenciados
R19	Medio		Corrupción de datos	Software ampliamente distribuido	8	10	12	Aceptable	
R20	Medio		Abuso de privilegios	Falta de controles para el cierre de sesión en terminales desatendidas	8	8	10	Tolerable	
R21	Bajo	Página Web de la Institución	Mal funcionamiento de software	Falta de control eficaz del cambio	3	1	16	Tolerable	La página web puede presentar deficiencias que no se consideran graves mientras no afecte a la transparencia de la información y las simulaciones de créditos

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R22	Bajo	Intranet de la Institución	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	4	3	12	Tolerable	Este sistema no es modificado con regularidad, por tanto, la falta de control de cambios no afecta el mantenimiento del sistema
R23	Medio	Sistema Operativo	Error en el uso	Falta de procedimientos para la introducción de software en sistemas operativos	9	8	16	Tolerable	El error en el uso del sistema operativo no afectan totalmente las actividades de la empresa
R24	Alto		Suplantación de identidad	Pobre gestión de claves secretas (passwords)	15	8	10	Intolerable	La suplantación de identidad puede exponer a acciones maliciosas
R25	Medio		Manipulación de software	Descarga y uso de software no controlados	9	4	12	Tolerable	La descarga de software y el uso no controlado, no afectan el sistema

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R26	Extremo	Sistema Financiero Integral	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	25	6	9	Intolerable	Este es el sistema principal de la financiera y debe mantener todos los procedimientos de software de manera ordenada para un fácil mantenimiento
R27	Bajo		Abuso de privilegios	Falta de pistas de auditoría	4	4	6	Tolerable	La falta de pistas de auditoría no afecta la continuidad del negocio
R28	Alto		Error en el uso	Falta de documentación	12	6	16	Tolerable	La falta de documentación podría dificultar o retrasar las operaciones pero no paraliza los procesos totalmente

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R29	Alto		Abuso de privilegios	Falta de procedimientos formales para la revisión de derechos de acceso (supervisión)	15	9	12	Intolerable	Los procedimientos de acceso deben ser revisados periódicamente ya que pueden afectar los procesos críticos de la organización
R30	Alto	Sistema SAP	Error en el uso	Uso incorrecto de software y hardware	15	9	12	Intolerable	El sistema SAP se usa para la gestión administrativa, por tanto, usarlo incorrectamente puede generar problemas en este aspecto
R31	Alto		Error en el uso	Interfaz de usuario complicada	15	6	12	Intolerable	Por ser un sistema usado en el backoffice, debe ser amigable para el usuario
R32	Extremo	Servicio a Equifax	Brechas en el mantenimiento de sistemas de información	Mantenimiento de servicios inadecuado	25	12	20	Intolerable	Servicio vital para el proceso de desembolso, no puede paralizarse

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R33	Alto		Error en el uso	Parametrización incorrecta	12	8	9	Intolerable	El servicio debe contar con una correcta parametrización dado que es consumido por uno de los procesos core de la empresa
R34	Medio		Procesamiento ilegal de datos	Servicios innecesarios habilitados	6	4	9	Tolerable	Pueden estar los servicios innecesarios habilitados siempre y cuando no sean consumidos por algún proceso core
R35	Alto	Servicio de correo electrónico	Error en el uso	Falta de políticas de uso de correo electrónico	15	12	20	Tolerable	El mal el uso del correo electrónico no afectan las actividades de la empresa
R36	Medio		Negociación de acciones	Falta de prueba del envió o la recepción de mensajes	6	4	9	Tolerable	Falta de pruebas en los servicios de mensajería podría afectar procesos procedimentales pero no afectan los procesos críticos de la organización

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R37	Extremo	Servicio de internet	Uso no autorizado de equipo	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería	25	16	20	Intolerable	El uso de internet es vital para el registro de transacciones, por tanto, usarlo para fines no laborales genera lentitud que afecta al negocio
R38	Extremo		Conexiones de red pública sin protección	Uso no autorizado del equipo	20	8	12	Intolerable	El uso no autorizado de equipos por conexiones públicas podría causar daños irreparables en la organización
R39	Extremo	Proceso de originación	Mal funcionamiento de software	Especificaciones poco claras o incompletas para desarrolladores	25	9	16	Intolerable	Este sistema es muy sensible a las modificaciones, por tanto, que no se especifiquen bien causa gran impacto
R40	Alto		Saturación del sistema de información	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	15	5	10	Intolerable	La disponibilidad de los sistemas que dan soporte al negocio no puede verse afectada, causaría importantes pérdidas

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R41	Extremo	Proceso de desembolso	Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia de acuerdos de niveles de servicio	25	15	20	Intolerable	El sistema que soporta este proceso es mantenido por un tercero con el cual es vital tener claro los términos de cumplimiento para no generar fallas en el proceso
R42	Bajo		Error en el uso	Falta de procedimientos para la introducción se software en sistemas operativos	4	4	6	Tolerable	Por el personal que es nuevo pueden surgir ciertos errores pero siempre son supervisados
R43	Medio		Abuso de privilegios	Falta o insuficiencia de pruebas de software	9	3	10	Tolerable	No existe un equipo especializado de pruebas pero si a nivel de los desarrolladores se realizan las pruebas básicas

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R44	Extremo	Proceso de cierre diario	Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador	20	15	16	Intolerable	El control de este proceso es vital y resulta importante contar con un reportes de las fallas que tengan los sistemas que le dan soporte
R45	Extremo		Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	20	9	12	Intolerable	La falta de monitoreo en las instalaciones podría ocasionar fallas en los procesos nocturnos que afectan a su vez a los procesos críticos de la organización
R46	Extremo	Proceso de cierre mensual	Procesamiento ilegal de los datos	Falta de mecanismos de monitoreo	20	12	16	Intolerable	El proceso de cierre diario es susceptible a ser alterado por el operador que lo ejecutar, lo que causaría inconsistencia en la información

VALORIZACIÓN DE RIESGOS									CÓDIGO: P011
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**PXI**	**APETITO**	**TOLERACIA**	**VALORIZACIÓN**	**COMENTARIO**
CÓDIGO	**NIVEL**								
R47	Alto		Uso no autorizado de equipo	Falta de revisiones de la gerencia en forma regular	15	5	10	Intolerable	La falta de revisión de la gerencia no afecta la continuidad del negocio
R48	Extremo	Proceso de cobranza	Abuso de los derechos	Defectos bien conocidos en el software	25	12	16	Intolerable	Errores en el software de cobranzas no son admisibles porque pueden causar fuertes pérdidas para la empresa
R49	Extremo	Backup de base de datos	Destrucción de equipo o medios	Procedimientos inadecuados de reclutamiento	25	12	16	Intolerable	El almacenamiento de los backup se realiza en un servidor que si no es usado de manera adecuada puede generar daños que lleve a perder la información guardada
R50	Alto		Manipulación de software	Falta de copias de respaldo	15	9	12	Intolerable	La falta de copias de respaldo de la información vital para la organización podría ocasionar parálisis temporal de algunos procesos críticos

Fase VI: Tratamiento del riesgo

Actividad 1: Seleccionar estrategias de tratamiento

A partir de la valorización del riesgo, se establece una estrategia.

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R1	Bajo	Computadora de escritorio	Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	Tolerable	Retener
R2	Bajo	Impresora	Robo de medios o documentos	Almacenamiento desprotegido	Aceptable	Retener
R3	Alto	Cableado Ethernet	Escucha subrepticia	Líneas de comunicación sin protección	Intolerable	Reducir
R4	Extremo		Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.	Intolerable	Reducir
R5	Medio	Firewall	Polvo, corrosión	Susceptible a humedad, polvo	Tolerable	Reducir
R6	Bajo		Falla de equipo de telecomunicaciones	Punto único de fallas	Aceptable	Retener

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R7	Medio		Espionaje remoto	Arquitectura insegura de la red	Tolerable	Reducir
R8	Alto	UPS	Falla de equipos	Falta de planes de continuidad	Intolerable	Evitar
R9	Bajo		Destrucción de equipamiento o medios	Falta de esquemas de reemplazo periódico	Aceptable	Retener
R10	Bajo		Sensibilidad a radiación electromagnética	Radiación electromagnética	Aceptable	Retener
R11	Extremo	Servidor BD Primario	Manipulación con software	Falta de copias de respaldo	Intolerable	Evitar
R12	Extremo		Robo de medios o documentos	Falta de autorización de instalaciones de procesamiento de información	Intolerable	Reducir
R13	Extremo	Servidor BD Secundario	Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	Intolerable	Reducir

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R14	Alto		Error en el uso	Falta de un eficiente control de cambios en la configuración	Intolerable	Evitar
R15	Medio	Servidor Correo	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación	Aceptable	Retener
R16	Alto		Falla de equipo de telecomunicaciones	Punto único de fallas	Intolerable	Evitar
R17	Medio		Espionaje remoto	Transferencia de contraseñas autorizadas	Intolerable	Reducir
R18	Medio	Licencias de software	Uso de software falsificado o copiado	Falta de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual	Tolerable	Reducir
R19	Medio		Corrupción de datos	Software ampliamente distribuido	Aceptable	Retener
R20	Medio		Abuso de privilegios	Falta de controles para el cierre de sesión en terminales desatendidas	Tolerable	Reducir
R21	Bajo	Página Web de la Institución	Mal funcionamiento de software	Falta de control eficaz del cambio	Tolerable	Retener

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R22	Bajo	Intranet de la Institución	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	Tolerable	Retener
R23	Medio	Sistema Operativo	Error en el uso	Falta de procedimientos para la introducción de software en sistemas operativos	Tolerable	Reducir
R24	Alto		Suplantación de identidad	Pobre gestión de claves secretas (passwords)	Intolerable	Evitar
R25	Medio		Manipulación de software	Descarga y uso de software no controlados	Tolerable	Reducir
R26	Extremo	Sistema Financiero Integral	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	Intolerable	Evitar
R27	Bajo		Abuso de privilegios	Falta de pistas de auditoría	Tolerable	Retener
R28	Alto		Error en el uso	Falta de documentación	Tolerable	Evitar
R29	Alto		Abuso de privilegios	Falta de procedimientos formales para la revisión de derechos de acceso (supervisión)	Intolerable	Reducir

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R30	Alto	Sistema SAP	Error en el uso	Uso incorrecto de software y hardware	Intolerable	Evitar
R31	Alto		Error en el uso	Interfaz de usuario complicada	Intolerable	Evitar
R32	Extremo	Servicio a Equifax	Brechas en el mantenimiento de sistemas de información	Mantenimiento de servicios inadecuado	Intolerable	Evitar
R33	Alto		Error en el uso	Parametrización incorrecta	Intolerable	Evitar
R34	Medio		Procesamiento ilegal de datos	Servicios innecesarios habilitados	Tolerable	Reducir
R35	Alto	Servicio de correo electrónico	Error en el uso	Falta de políticas de uso de correo electrónico	Tolerable	Evitar
R36	Medio		Negociación de acciones	Falta de prueba del envió o la recepción de mensajes	Tolerable	Reducir
R37	Extremo	Servicio de internet	Uso no autorizado de equipo	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería	Intolerable	Evitar
R38	Extremo		Conexiones de red pública sin protección	Uso no autorizado del equipo	Intolerable	Evitar

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R39	Extremo	Proceso de originación	Mal funcionamiento de software	Especificaciones poco claras o incompletas para desarrolladores	Intolerable	Reducir
R40	Alto		Saturación del sistema de información	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Intolerable	Evitar
R41	Extremo		Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia de acuerdos de niveles de servicio	Intolerable	Evitar
R42	Bajo		Error en el uso	Falta de procedimientos para la introducción se software en sistemas operativos	Tolerable	Retener
R43	Medio		Abuso de privilegios	Falta o insuficiencia de pruebas de software	Tolerable	Reducir
R44	Extremo		Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador	Intolerable	Retener
R45	Extremo		Abuso de privilegios	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	Intolerable	Evitar

TRATAMIENTO DE RIESGOS						CÓDIGO: P012
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.						
RIESGO		**ACTIVO**	**AMENAZA**	**VULNERABILIDAD**	**VALORIZACIÓN**	**ESTRATEGIA**
CÓDIGO	**NIVEL**					
R46	Extremo		Procesamiento ilegal de los datos	Falta de mecanismos de monitoreo	Intolerable	Evitar
R47	Alto		Uso no autorizado de equipo	Falta de revisiones de la gerencia en forma regular	Intolerable	Evitar
R48	Extremo		Abuso de los derechos	Defectos bien conocidos en el software	Intolerable	Evitar
R49	Extremo		Destrucción de equipo o medios	Procedimientos inadecuados de reclutamiento	Intolerable	Evitar
R50	Alto		Manipulación de software	Falta de copias de respaldo	Intolerable	Reducir

Actividad 2: Proponer planes de acción

Para los riesgos extremos y altos se establece un plan de acción.

SEGUIMIENTO DE PLANES DE ACCIÓN							CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
CODIGO RIESGO	**NIVEL RIESGO**	**ESTRATEGIA**	**PLAN DE ACCION**	**DESCRIPCION**	**PRESUPUESTO**	**FECHA OBJETIVO**	**RESPONSABLE**
R3	Alto	Reducir	Manual de especificaciones técnicas de cableado	Elaborar un manual de especificaciones técnicas de los requisitos de seguridad mínimos para proteger las redes de comunicaciones	s/.0.00	12/01/2018	Jefe de producción de sistemas
R4	Extremo	Reducir	Mantenimiento de equipos	Elaborar planes de mantenimiento de equipos periódicamente	s/.1500	15/02/2018	Jefe de producción de sistemas
R8	Alto	Evitar	Plan de recuperación de servicios de TI	Ante cualquier falla del servidor primario, se activará el plan de recuperación como respaldo el servidor secundario	s/.0.00	26/03/2018	Gerencia de sistemas
R11	Extremo	Evitar	Políticas de backup	Actualizar políticas de copias de respaldo del servidor primario y capacitación a operadores	s/.0.00	05/01/2018	Administrador de base de datos

SEGUIMIENTO DE PLANES DE ACCIÓN							CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
CODIGO RIESGO	**NIVEL RIESGO**	**ESTRATEGIA**	**PLAN DE ACCION**	**DESCRIPCION**	**PRESUPUESTO**	**FECHA OBJETIVO**	**RESPONSABLE**
R12	Extremo	Reducir	Políticas de autorización de instalación de pases	Elaborar políticas de autorización para instalación de pases a producción	s/.0.00	26/01/2018	Jefe de desarrollo
R13	Extremo	Reducir	Políticas de monitoreo de procesos de información críticos	Elaborar políticas de monitoreo de procesos de información críticos	s/.0.00	10/01/2018	Jefe de aplicaciones
R14	Alto	Evitar	Plan de contingencia para la recuperación de configuraciones de servidores	Elaborar plan de contingencia para la recuperación de configuraciones de servidores	s/.0.00	23/02/2018	Jefe de producción de sistemas
R16	Alto	Evitar	Políticas de reporte de fallas en equipo de telecomunicaciones	Elaborar políticas de reporte de fallas en equipo de telecomunicaciones	s/.0.00	15/03/2018	Jefe de producción de sistemas
R24	Alto	Evitar	Documento de mejores prácticas para contraseñas	Elaborar un documento estableciendo os estándares mínimos establecidos para aceptar una contraseña segura	s/.0.00	15/04/2018	Jefe de producción de sistemas
R26	Extremo	Evitar	Procedimiento de control de cambios	Elaborar un procedimiento de control de cambios para una correcta control de las fuentes	s/.0.00	15/01/2018	Jefe de producción de sistemas

SEGUIMIENTO DE PLANES DE ACCIÓN							CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
CODIGO RIESGO	**NIVEL RIESGO**	**ESTRATEGIA**	**PLAN DE ACCION**	**DESCRIPCION**	**PRESUPUESTO**	**FECHA OBJETIVO**	**RESPONSABLE**
R28	Alto	Evitar	Proyecto de elaboración de documentación de procesos críticos y principales de la organización	Elaborar un proyecto para la documentación de procesos críticos	s/.0.00	23/02/2018	Área de procesos
R29	Alto	Reducir	Procedimientos formales para la revisión de derechos de acceso	Elaborar un procedimiento para la revisión de derechos de acceso	s/.0.00	23/02/2018	Oficial de seguridad de la información
R30	Alto	Evitar	Plan de entrenamiento y capacitación para el personal de la organización	Realizar capacitaciones al personal que maneja la herramienta para evitar errores de usuario	s/.0.00	23/05/2018	Gerencia de sistemas Gerencia de RRHH
R31	Alto	Evitar	Plan de entrenamiento y capacitación para el personal de la organización	Realizar capacitaciones al personal que maneja la herramienta para evitar errores de usuario	s/.0.00	23/02/2018	Gerencia de sistemas Gerencia de RRHH
R32	Extremo	Evitar	Contingencia para Equifax	Contar con una base de contingencia para cuando no se pueda acceder el servicio de Equifax	s/950.00	15/02/2018	Jefe de desarrollo

SEGUIMIENTO DE PLANES DE ACCIÓN							CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
CODIGO RIESGO	**NIVEL RIESGO**	**ESTRATEGIA**	**PLAN DE ACCION**	**DESCRIPCION**	**PRESUPUESTO**	**FECHA OBJETIVO**	**RESPONSABLE**
R33	Alto	Evitar	Capacitación a personal de producción sobre servicios externos	Actualización de conocimientos sobre soporte de los servicios externos	s/.1000	15/04/2018	Jefe de producción de sistemas
R35	Alto	Evitar	Políticas de uso de correo electrónico	Establecer políticas de uso de correo electrónico	s/.0.00	15/03/2018	Jefe de producción de sistemas
R37	Extremo	Evitar	Políticas para el uso correcto de medios de comunicación y mensajería	Elaborar políticas para el uso correcto de medios de comunicación y mensajería	s/.0.00	23/02/2018	Oficial de seguridad de la información
R38	Extremo	Evitar	Políticas para el uso no autorizado de equipos y conexiones a redes públicas	Elaborar políticas para el uso no autorizado de equipos y conexiones a redes públicas	s/.0.00	23/02/2018	Oficial de seguridad de la información
R39	Extremo	Reducir	Mecanismo para asegurar claridad en documento de especificaciones	Coordinar con procesos y funcionales para que sean el primer filtro y se tengan claras y definidas las especificaciones antes de enviar a desarrollo	s/.0.00	15/01/2018	Jefe de control y presupuesto
R40	Alto	Evitar	Pautas para la gestión adecuada de la red	Documentar las buenas prácticas para la gestión adecuada de la red	s/.0.00	12/04/2018	Jefe de producción de sistemas

SEGUIMIENTO DE PLANES DE ACCIÓN							CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
CODIGO RIESGO	**NIVEL RIESGO**	**ESTRATEGIA**	**PLAN DE ACCION**	**DESCRIPCION**	**PRESUPUESTO**	**FECHA OBJETIVO**	**RESPONSABLE**
R41	Extremo	Evitar	Actualización de contratos y/o adendas	Establecer niveles de servicio con proveedores para atención oportuna ante alguna eventualidad	s/.0.00	07/05/2018	Jefe de desarrollo Jefe de control y presupuesto
R44	Extremo	Retener	Proyecto de inserción de log	Proyecto de inserción de log para monitoreo en todos los procesos de cierre	S/. 2,000	12/01/2018	Jefe de producción de sistemas
R45	Extremo	Evitar	Procedimiento para el monitoreo de instalaciones de procesamiento de información	Elaborar un procedimiento para el monitoreo de instalaciones de procesamiento de información	s/.0.00	15/01/2018	Jefe de producción de sistemas
R46	Extremo	Evitar	Procedimiento de monitoreo a la base de datos	Elaborar un procedimiento de monitoreo contaste a la base de datos	s/.0.00	15/01/2018	Jefe de producción de sistemas
R47	Alto	Evitar	Programar revisiones gerenciales del uso y manipulación de equipos críticos	Elaborar un programa de revisión gerencial	s/.0.00	30/04/2018	Jefe de producción de sistemas

SEGUIMIENTO DE PLANES DE ACCIÓN							CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.							
CODIGO RIESGO	**NIVEL RIESGO**	**ESTRATEGIA**	**PLAN DE ACCION**	**DESCRIPCION**	**PRESUPUESTO**	**FECHA OBJETIVO**	**RESPONSABLE**
R48	Extremo	Evitar	Documento de escenarios de pruebas	Contar documento de escenarios de pruebas elaborados por el analista funcional en coordinación con el usuario	s/.0.00	09/02/2018	Jefe de control de calidad
R49	Extremo	Evitar	Programar revisiones gerenciales del uso y manipulación de equipos críticos	Elaborar un programa de revisión gerencial	s/.0.00	26/03/2018	Jefe de producción de sistemas
R50	Alto	Reducir	Documento de escenarios de pruebas	Contar documento de escenarios de pruebas elaborados por el analista funcional en coordinación con el usuario	s/.0.00	28/02/2018	Jefe de control de calidad

PLAN DE ACCIÓN	CÓDIGO: P013
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.	
PLAN DE RECUPERACIÓN DE SERVICIOS DE TI	
Descripción	Cumple con la finalidad de minimizar los efectos de un desastre y que la institución sea capaz de mantener y estabilizar en un tiempo prudente sus operaciones críticas del negocio.
Alcance	La recuperación se realizará en el servidor secundario definido por la financiera.
Objetivos	* Proteger los recursos de la financiera. * Salvaguardar los registros vitales. * Garantizar la disponibilidad de los principales servicios de TI. * Minimizar el grado de interrupción, el daño e impacto de un incidente en los productos y servicios de la financiera. * Proporcionar mecanismos para una rápida restauración de las operaciones tecnológicas.
Roles, responsabilidades y autoridades	* Coordinador de Recuperación de TI. * Coordinador de Infraestructura Tecnológica. * Coordinador de Sistemas de Información. * Coordinador de Soporte Técnico. * Coordinador de Red. * Coordinador de Seguridad de la Información.
Riesgos asociados	R26
Nivel del riesgo	Extremo
Aplicaciones de los procesos	Sistema Financiero Integrado.
Registros vitales	* Generación de créditos. * Registro de clientes. * Registro de contabilidad. * Registro de líneas de crédito.
Recursos necesarios	* Servidores. * Equipos de comunicación (switch, router, firewall).
Procedimiento de recuperación ante emergencias	* Evaluación de daños. * Notificar el daño. * Activar servidor secundario. * Recuperar comunicación en la oficina principal. * Recuperar equipos. * Recuperar base de datos y aplicaciones. * Recuperar servicios de red.
Indicador clave de riesgo	* Tiempo de recuperación del servicio.

Fase VII: Monitoreo y revisión

Los planes de acción definidos se monitorean para controlar su cumplimiento.

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R3	Alto	Manual de especificaciones técnicas de cableado	Elaborar un manual de especificaciones técnicas de los requisitos de seguridad mínimos para proteger las redes de comunicaciones.	12/01/2018	31/01/2018	100%	s/.0.00	s/.0.00	Concluido
R4	Extremo	Mantenimiento de equipos	Elaborar planes de mantenimiento de equipos periódicamente	15/02/2018	31/01/2018	100%	s/.1500	s/.1300	Concluido
R8	Alto	Plan de recuperación de servicios de TI	Ante cualquier falla del servidor primario, se	26/03/2018	15/03/2018	100%	s/.0.00	s/.0.00	Concluido

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
			activará el plan de recuperación como respaldo el servidor secundario						
R11	Extremo	Políticas de backup	Actualizar políticas de copias de respaldo del servidor primario y capacitación a operadores	05/01/2018	31/01/2018	100%	s/.0.00	s/.0.00	Concluido
R12	Extremo	Políticas de autorización de instalación de pases	Elaborar políticas de autorización para instalación de pases a producción	26/01/2018	31/01/2018	100%	s/.0.00	s/.0.00	Concluido
R13	Extremo	Políticas de monitoreo de procesos de información críticos	Elaborar políticas de monitoreo de procesos de información críticos	10/01/2018	--	100%	s/.0.00	--	Pendiente

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R14	Alto	Plan de contingencia para la recuperación de configuraciones de servidores	Elaborar plan de contingencia para la recuperación de configuraciones de servidores	23/02/2018	28/02/2018	100%	s/.0.00	s/.0.00	Concluido
R16	Alto	Políticas de reporte de fallas en equipo de telecomunicaciones	Elaborar políticas de reporte de fallas en equipo de telecomunicaciones	15/03/2018	--	80%	s/.0.00	s/.0.00	En Ejecución
R24	Alto	Documento de mejores prácticas para contraseñas	Elaborar un documento estableciendo os estándares mínimos establecidos para aceptar una contraseña segura	15/04/2018	31/04/2018	100%	s/.0.00	s/.0.00	Concluido

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R26	Extremo	Procedimiento de control de cambios	Elaborar un procedimiento de control de cambios para una correcta control de las fuentes	15/01/2018	28/02/2018	100%	s/.0.00	s/.0.00	Concluido
R28	Alto	Proyecto de elaboración de documentación de procesos críticos y principales de la organización	Elaborar un proyecto para la documentación de procesos críticos	23/02/2018	31/03/2018	100%	s/.0.00	s/.0.00	Concluido
R29	Alto	Procedimientos formales para la revisión de derechos de acceso	Elaborar un procedimiento para la revisión de derechos de acceso	23/02/2018	28/02/2018	100%	s/.0.00	s/.0.00	Concluido
R30	Alto	Plan de entrenamiento y capacitación para el personal de la organización	Realizar capacitaciones al personal que maneja la herramienta para evitar errores de usuario	23/05/2018	09/05/2018	100%	s/.0.00	s/.0.00	Concluido

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R31	Alto	Plan de entrenamiento y capacitación para el personal de la organización	Realizar capacitaciones al personal que maneja la herramienta para evitar errores de usuario	23/02/2018	09/03/2018	100%	s/.0.00	--	Concluido
R32	Extremo	Contingencia para Equifax	Contar con una base de contingencia para cuando no se pueda acceder el servicio de Equifax	15/02/2018	--	50%	s/950.00	s/500.00	En Ejecución
R33	Alto	Capacitación a personal de producción sobre servicios externos	Actualización de conocimientos sobre soporte de los servicios externos	15/04/2018	--	100%	s/.1000	--	Pendiente
R35	Alto	Políticas de uso de correo electrónico	Establecer políticas de uso de correo electrónico	15/03/2018	--	65%	s/.0.00	s/.0.00	En Ejecución

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R37	Extremo	Políticas para el uso correcto de medios de comunicación y mensajería	Elaborar políticas para el uso correcto de medios de comunicación y mensajería	23/02/2018	--	100%	s/.0.00	--	Pendiente
R38	Extremo	Políticas para el uso no autorizado de equipos y conexiones a redes públicas	Elaborar políticas para el uso no autorizado de equipos y conexiones a redes públicas	23/02/2018	--	90%	s/.0.00	s/.0.00	En Ejecución
R39	Extremo	Mecanismo para asegurar claridad en documento de especificaciones	Coordinar con procesos y funcionales para que sean el primer filtro y se tengan claras y definidas las especificaciones antes de enviar a desarrollo	15/01/2018	--	100%	s/.0.00	--	Pendiente

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R40	Alto	Pautas para la gestión adecuada de la red	Documentar las buenas prácticas para la gestión adecuada de la red	12/04/2018	--	40%	s/.0.00	s/.0.00	En Ejecución
R41	Extremo	Actualización de contratos y/o adendas	Establecer niveles de servicio con proveedores para atención oportuna ante alguna eventualidad	07/05/2018	--	100%	s/.0.00	--	Pendiente
R44	Extremo	Proyecto de inserción de log	Proyecto de inserción de log para monitoreo en todos los procesos de cierre	12/01/2018	--	30%	S/. 2,000	s/.600.00	En Ejecución
R45	Extremo	Procedimiento para el monitoreo de instalaciones de procesamiento de información	Elaborar un procedimiento para el monitoreo de instalaciones de procesamiento de información	15/01/2018	15/03/2018	100%	s/.0.00	s/.0.00	Concluido

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R46	Extremo	Procedimiento de monitoreo a la base de datos	Elaborar un procedimiento de monitoreo contaste a la base de datos	15/01/2018	30/03/2018	100%	s/.0.00	s/.0.00	Concluido
R47	Alto	Programar revisiones gerenciales del uso y manipulación de equipos críticos	Elaborar un programa de revisión gerencial	30/04/2018	23/04/2018	100%	s/.0.00	s/.0.00	Concluido
R48	Extremo	Documento de escenarios de pruebas	Contar documento de escenarios de pruebas elaborados por el analista funcional en coordinación con el usuario	09/02/2018	15/03/2018	100%	s/.0.00	s/.0.00	Concluido
R49	Extremo	Programar revisiones gerenciales del uso y manipulación de equipos críticos	Elaborar un programa de revisión gerencial	26/03/2018	--	50%	s/.0.00	s/.0.00	En Ejecución

MONITOREO Y REVISIÓN DE PLANES DE ACCIÓN									CÓDIGO: P014
Elaborado por: Analista de riesgo operacional. Revisado por: Gerente de riesgos. Aprobado por: Comité de riesgos.									
RIESGO		**PLAN DE ACCION**	**DESCRIPCION**	**FECHA OBJETIVO**	**FECHA CULMINACIÓN**	**% DE AVANCE**	**PRESUPUESTO ASIGNADO**	**PRESUPUESTO EJECUTADO**	**ESTADO**
CÓDIGO	**NIVEL**								
R50	Alto	Documento de escenarios de pruebas	Contar documento de escenarios de pruebas elaborados por el analista funcional en coordinación con el usuario	28/02/2018	--	50%	s/.0.00	s/.0.00	En Ejecución

Fase VIII: Comunicación y Consulta

Como una retroalimentación, se reciben comunicaciones de factores de riesgos que permiten la mejora continua.

COMUNICACIÓN DE RIESGOS Y CONSULTAS		CÓDIGO: P016
Elaborado por: Vendedor. Revisado por: Gerente de tienda. Aprobado por: Gerente de riesgos.		
TIPO DE COMUNICACIÓN	**Factor de riesgo**	Mejora
COMUNICANTE		
NOMBRE	Roxana Vilchez Torres	
OFICINA	Tienda Chiclayo	
FECHA	28-12-2017	
DETALLE	Se detectó caída del sistema de ventas cuando se realizaba un registro a las 09:50am. Se trata de la venta de un equipo LG, además el precio que se mostraba no corresponde con el catálogo físico que se nos entregó.	
DOCUMENTOS ADJUNTOS	Capturas de pantallas del sistema.	