UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

ESCUELA DE POSTGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE

MODELO DE GESTIÓN DE RIESGOS DE TI PARA EL CUMPLIMIENTO DE LAS EXIGENCIAS DE LA SBS EN SECTOR MICROFINANCIERO DE CHICLAYO

TESIS

PRESENTADO PARA OPTAR EL GRADO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE

PRESENTADO POR:

ROBERTO CARLOS SANTA CRUZ ACOSTA

ASESOR:

M.SC. ERNESTO KARLOS CELI AREBALO

Lambayeque – Perú
2018

Modelo de Gestión de Riesgos de TI para el cumplimiento de las exigencias de la SBS en el sector Microfinanciero en Chiclayo

Ing. Carlos Santa Cruz Acosta
Autor

M.Sc. Ernesto Karlo Arevalo Celi
Asesor

Presentado a la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el grado de MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DE SOFTWARE.

APROBADO POR

Dr. Edward Haro Maldonado
Presidente del jurado

Mg. Jesús Olavarría Paz
Secretario del Jurado

Mg. Martin Ampuero Pasco
Vocal del Jurado

Lambayeque – Perú
2018

DEDICATORIA

Dedico este trabajo de investigación a mi esposa Celeste por su paciencia y comprensión en todos estos días de investigación, a mis hijos Cristofer y Xiarita; quienes son el motivo para seguir avanzando y poco a poco lograr mis objetivos. A mis padres José y Hermis quienes siempre me apoyaron de una forma incondicional, dándome amor e inculcándome valores para ser una persona de bien.

AGRADECIMIENTO

Agradezco a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mis padres, por ser los pilares más importantes y por demostrarme siempre su cariño y apoyo incondicional para ser de mí una mejor persona.

A mi esposa e hijos, por estar presentes no solo en esta etapa de mi vida, sino en todo momento ofreciéndome su amor y calidez de familia a la cual amo.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN

La finalidad de esta investigación es describir como debe ser un modelo de gestión de riesgos de tecnologías de Información contemplando la gestión de la continuidad de los procesos del negocio y así asegurar la eficacia y efectividad de los sistemas de Gestión de la seguridad de la información en el sector Microfinanciero de Chiclayo.

Así como la estrategia para tener la información que se requiere para la toma de decisiones y poder implementar loa controles de TI. La falta de metodología adecuada para dar soporte al sector Microfinanciero de Chiclayo cumpliendo con las exigencias de la SBS.

Se demostró modelo de gestión de riesgos de TI para el cumplimiento de las exigencias de la SBS en el sector Microfinanciero en Chiclayo implementado, tomando como referencia los estándares se puede logra mayor efectividad para determinar los diferentes riesgos en los diferentes activos de TI, en las etapas de evaluación tratamiento, a través de la implementación y seguimiento de controles considerando los requerimientos mínimos de la SBS

PALABRAS CLAVES

Modelo Gestión de Riesgos, Gestión de la seguridad de la información. Exigencia de la SBS

ABSTRACT

The purpose of this research is to describe how an information technology risk management model should be considered, considering the continuity management of business processes and thus ensure the effectiveness and effectiveness of information security management systems in the Microfinance sector of Chiclayo.

As well as the strategy to have the information that is required for decision making and to be able to implement IT controls. The lack of adequate methodology to support the microfinance sector of Chiclayo fulfilling the SBS requirements.

An IT risk management model was demonstrated for compliance with the SBS requirements in the Microfinance sector in Chiclayo implemented, taking the standards as a reference, it is possible to achieve greater effectiveness in determining the different risks in the different IT assets, in the stages of treatment evaluation, through the implementation and monitoring of controls considering the minimum requirements of the SBS

KEYWORDS:
Risk Management Model, Management of information security. Demand of the SBS

INTRODUCCIÓN

En los últimos años las entidades Microfinacieras en Chiclayo ha registrado un rápido y muy significante crecimiento en el sistema financiero, junto con los avances de la tecnología, donde los riesgos forman parte inherente, debido a los cambios e incertidumbres propios de la actividad empresarial por consecuente se incrementan los riesgos. Por lo mismo las Microfinancieras tiene que encontrar la forma más adecuada de absolver y mitigar los riesgos que se les presenten, en la cual las TI toma un papel importante.

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.

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 Chiclayo, existe un número significativo de instituciones microfinancieras operando. Todas ellas cuentan con un área de riesgos que analiza los distintos tipos de riesgos, según las exigencias de 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. Estas situaciones de riesgo para las organizaciones, pueden evitarse realizando una adecuada gestión de riesgos que de soporte a la continuidad del negocio.

El objetivo general de esta investigación es, contribuir a la continuidad del negocio de las microfinancieras de Chiclayo, mediante el desarrollo de un modelo de Gestión de Riesgos de TI.

I. ANÁLISIS DEL OBJETO DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Actualmente en las microfinancieras de Chiclayo 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 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.

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.

1.2. FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede mejorar la gestión de riesgos de TI de acuerdo con las exigencias de la SBS, en el sector microfinanciero en Chiclayo?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Expuesto que la presente tesis tenemos como objetivo general el Mejorar la gestión de riesgos de TI en las empresas microfinancieras de la ciudad de Chiclayo cumpliendo con las exigencias de la SBS, por medio de la implementación de un modelo de gestión de riesgos de TI;

1.3.2. OBJETIVOS ESPECÍFICOS

a. Desarrollar un modelo general para la gestión de riesgos de TI, que considere las etapas de evaluación y tratamiento de los riesgos
b. Definir una metodología para implementar el modelo general para la gestión de riesgos de TI
c. Evaluar el modelo y metodología propuesta para la gestión de riesgos de TI aplicando el método Delphi

1.4. MATERIALES Y MÉTODOS

1.4.5. DISEÑO DE INVESTIGACIÓN

De acuerdo al propósito del estudio el diseño de la investigación es observacional, porque dado las limitaciones que se tiene para acceder a la infraestructura tecnológica y a la información, es decir no es posible manejar la variable independiente; se opta por observar los efectos del modelo propuesto a través de las evaluaciones que realicen los actores directos de los procesos relacionados con la investigación al diseño y aplicabilidad del modelo propuesto.

1.4.6. HIPÓTESIS

Con la implementación de un modelo de gestión de riesgos TI para el cumplimiento exigencias de la SBS, se mejorará la gestión de riesgos relacionados con TI en las empresas microfinancieras de la ciudad de Chiclayo

1.4.7. DISEÑO DE CONTRASTACIÓN

El modelo lógico de contrastación es del tipo cuasi experimental del tipo

G: X O

Dónde:

- el grupo de casos ha sido seleccionado intencionalmente y evaluado con una sola prueba: post prueba

- Se establece una línea base previa de tratamiento y se verifica equivalencias utilizando medias o desviaciones (grupo de control no equivalente)

  X: Modelo de gestión de riesgos de TI para el cumplimiento de las exigencias de la SBS en el sector microfinanciero en Chiclayo.

  O: La Observación postest consistirá en un cuestionario enviado al panel de personas seleccionadas para asignar pesos a los factores, variables y niveles del modelo propuesto, que se aplicará en el caso de estudio, con la finalidad de evaluar la efectividad del diseño y efectividad de la operación del modelo de gestión de riesgos propuesto (X).

1.4.7.1. Variables

a. Variable Independiente:
   Modelo de gestión de riesgos de TI para el cumplimiento de las exigencias de la SBS en el sector microfinanciero en Chiclayo.
b. Variable Dependiente:
   Gestión de riesgos relacionados con TI.

1.4.7.2. Variables – Operacionalización

Tabla N° 01: Operacionalización de variables

Variable	Perspectiva	Dimensión	Indicador
Gestión de riesgos de TI	efectividad del diseño del modelo	Estructuración de la metodología de análisis y tratamiento de riesgos	Efectividad en la definición de los riesgos de TI según las categorías de información
			Nivel de integración del modelo en la gestión de riesgos corporativo
			Grado de concientización
		Gobierno de los riesgos de TI	Cumplimiento normativo de las variables exigidas por la SBS
			Efectividad en la evaluación de los componentes del modelo de gestión de TI: amenazas, vulnerabilidades, impactos, frecuencias
			Efectividad del monitoreo de las actividades de gestión de riesgos de TI
			Tiempo de recuperación de incidentes (RTO)
	efectividad de la operación del modelo	Análisis y tratamiento de riesgos	Nivel de aplicabilidad del proceso implantado en el modelo propuesto para evaluar los riesgos de TI
			Efectividad los niveles de riesgos inherentes de TI
			Efectividad de la implantación de controles y seguimiento de las brechas de seguridad
		Gobierno de los riesgos de TI	Grado de satisfacción por la información resultante del modelo
			Grado de satisfacción del modelo para la toma de decisiones en relación a las inversiones de los controles de seguridad

1.4.8. POBLACIÓN Y MUESTRA

Dado que el diseño de contrastación de la hipótesis es cuasi experimental, entonces la muestra ha sido seleccionada intencionalmente dado que son las personas de las microfinancieras de Chiclayo, que están directamente relacionados y que tienen la capacidad y autoridad para cumplir con las funciones de:

- Jefatura de TI
- Jefatura de la Unidad de Riesgos
- Oficialía de Seguridad de TI y de la Información
- Jefatura de la Unidad de Continuidad de negocio
- Auditor interno

La intención es que las personas que cumplen estas funciones sean los que evalúen el modelo de gestión propuesto.

1.4.9. MÉTODOS Y TÉCNICAS RECOLECCIÓN DE DATOS

En la investigación se emplearán múltiples técnicas e instrumentos de recolección de información: documentación (fichas de revisión de datos), entrevistas, encuestas y observaciones directas.

- Documentación, se revisarán los documentos estratégicos, administrativos y legales pertenecientes a las Microfinancieras de Chiclayo, materia de estudio de caso, y se elaborarán fichas de revisión de datos, de cada documento, conteniendo información primordial de cada uno de ellos. Los documentos que se revisarán serán (en el caso de que existiesen):

  De la Jefatura de Tecnologías de la Información y Organización y Métodos

  a. Plan estratégico de TI
  b. Plan anual de TI
  c. Sistema de Gestión de Seguridad de la Información
  d. Manual de gestión de riesgos operativos de TI, con sus correspondientes informes y plan de pruebas

- Entrevistas, las entrevistas servirán para obtener información de los procedimientos actuales para la evaluación y seguimiento de los controles implantados para la protección y salvaguarda de los activos tecnológicos considerados en esta investigación. Serán conducidas en base a un protocolo determinado en los formatos tipo checklist preparados para este efecto (Ver Anexo N° 02). Se aplicará para el diagnóstico de los controles existentes. Básicamente se entrevistará, según sea el caso,

- Observación directa, para complementar el llenado de los formatos del Anexo N° 02 en el diagnóstico de los controles existentes.

- Encuestas. Se realizarán encuestas escritas, aplicando la técnica Delphi (juicio de expertos), donde los funcionarios indicados en las entrevistas, evaluarán la efectividad del diseño y de operación del modelo de gestión de riesgos de TI

propuesto. Se ha seleccionado a los funcionarios indicados porque tienen la capacidad y autoridad para gestionar la seguridad de TI y de la información en las diferentes áreas de las Microfinancieras de Chiclayo. La estructura de la encuesta se muestra en el Anexo N° 01. Se aplicará en el post test**.**

1.4.10. TÉCNICAS DE PROCESAMIENTO DE DATOS

Para el procesamiento de análisis de los datos se utilizó Microsoft Excel, a través del cual se obtuvieron los resultados de las encuestas.

1.4.11. METODOLOGÍA

El modelo de Gestión de Riesgo propuesto, permitió determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Para lograr ello, se identifica y evalúa los diferentes componentes, que los diferentes estándares y metodologías estudiadas, establecen como básicos en la gestión de riesgos de TI, como: los activos de TI, las amenazas, las vulnerabilidades, los impactos y las probabilidades; y así identificar, tanto el nivel de riesgo existente como el nivel de riesgo aceptable de la entidad financiera.

Finalmente, se evalúa y establece las recomendaciones sobre la eficiencia y madurez de los controles que éste tipo organizaciones implementan para gestionar sus riesgos de TI.

Así mismo, en el proceso de construcción de la propuesta, se ha tomado como referencia las exigencias de la Superintendencia de Banca y Seguros, que establece los lineamientos para la Gestión de Riesgos de TI de éste tipo de empresas, las mismas que forman parte anexa de este trabajo de investigación (Ver Anexo N° 8).

En resumen, para el diseño del modelo de gestión de riesgos propuesto se ha tomado como referencia las políticas de seguridad, normas y reglas exigidas a las entidades financieras en el Perú por parte de su ente supervisores como es la SBS; así como de los estándares y metodologías que se han tomado como referencia.

El modelo propuesto contiene cuatro fases, que abarcan las etapas de evaluación de riesgos y tratamiento de los mismos:

1. Análisis de riesgos: donde se determinan los componentes de un sistema de TI que requiere protección y que le dan soporte a los procesos críticos. Esta etapa también contempla la identificación y estimación de sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
2. Clasificación de los riesgos: donde se determina si los riesgos intrínseco y efectivo encontrados y sí los riesgos restantes o residuales son aceptables.
3. Implementación de controles: aquí se define e implementa las medidas de protección como controles o salvaguardas.
4. Control de eficiencia y madurez: analiza el funcionamiento, la efectividad y el cumplimiento de las medidas de protección para determinar y ajustar las medidas deficientes y sancionar el incumplimiento.

El modelo general de gestión de riesgos propuesto y la metodología para su aplicación están resumidos en los siguientes gráficos:

Gráfico N° 01: Modelo general del modelo de análisis de riesgos propuesto

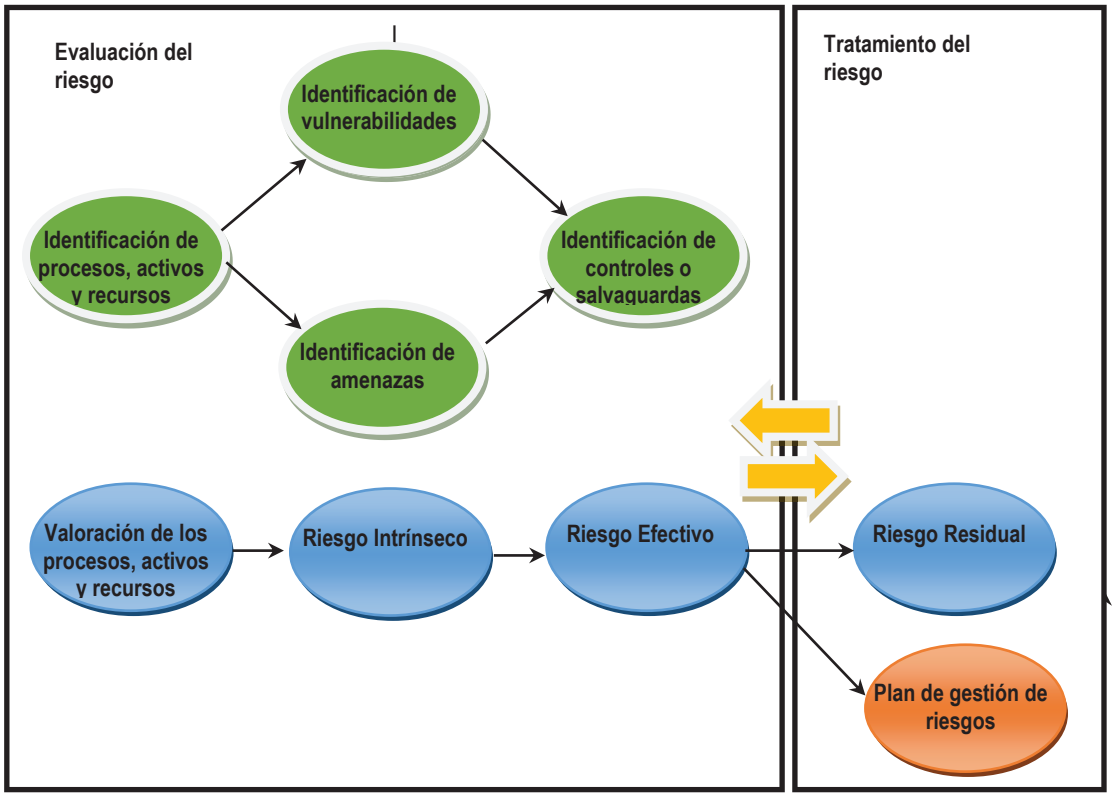
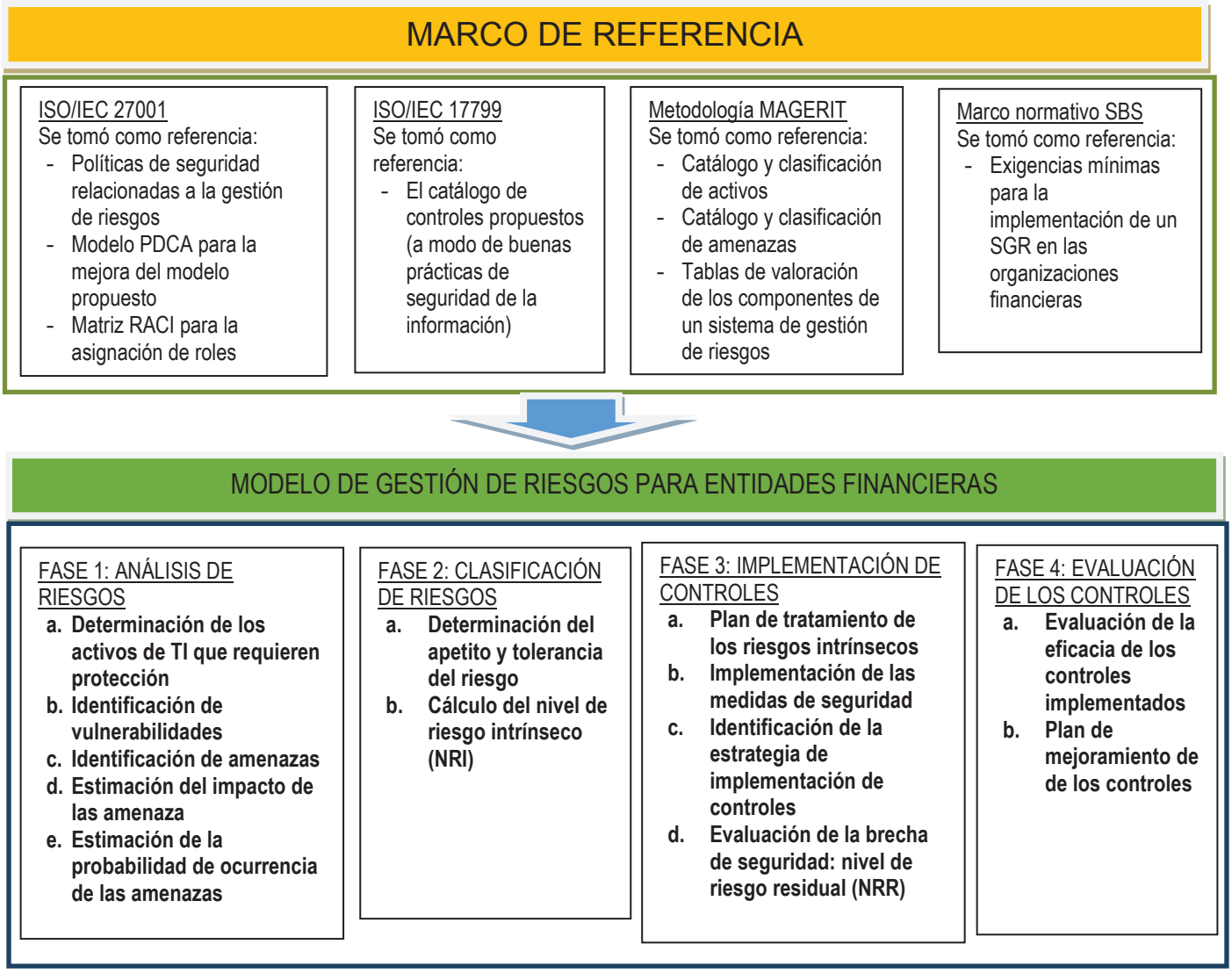


Gráfico N° 02: Metodología para la aplicación del modelo de análisis de riesgos propuesto



1.4.11.1. Fase 1: Análisis de riesgos de TI

En esta fase se identificarán los riesgos de seguridad de la información que podrían impedir que la organización financiera no logre sus objetivos, determinando su magnitud e identificando las áreas que requieren medidas de salvaguarda o controles en función del riesgo detectado: intrínseco y efectivo.

Esta fase contempla las siguientes actividades y tareas:

A. Identificación de activos de TI y definición de su criticidad
B. Identificación de amenazas por activo
C. Identificación de vulnerabilidades
D. Estimación del impacto de las amenazas
E. Estimación de la probabilidad de ocurrencia de la amenazas

A. Identificación de activos de TI y definición de su criticidad

Esta actividad busca identificar los activos relevantes dentro de los procesos críticos identificados de la entidad, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

Tabla N° 02: Ficha técnica de la actividad identificación de activos de TI y definición de su criticidad

Tarea: Identificación de activos de TI		
Objetivo: Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados.		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Descripción de los procesos críticos del negocio - Inventario de servicios y equipos prestados por el sistema - Inventario de equipamiento físico - Locales y sedes de la organización - Caracterización funcional de los puestos de trabajo	- Inventario de activos de TI a evaluar - Clasificación de los activos de TI	- Diagramación de flujo de datos y diagramación de procesos de negocio - Entrevistas con los propietarios de los activos de TI - Reuniones con los responsables del uso y mantenimiento de los activos de TI - Utilizar Tabla de referencia para el inventario y clasificación de activos de TI (Ver anexo N° 03)
Tarea: Definición de la criticidad de los activos de TI		
Objetivos Identificar las dimensiones de la información relacionadas con cada activo de TI Valorar el coste que para la organización de la no disponibilidad de cada activo de TI		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Inventario de activos de TI - Descripción de los procesos críticos del negocio: - Diagramas de flujo de datos	- Modelo de valor: Informe del valor de los activos de TI	- Entrevistas con los propietarios de los activos de TI - Reuniones con los responsables del uso y mantenimiento de los activos de TI - Valoración Delphi - Usar Tablas de referencia para la valoración de la criticidad de los activos de TI (ver Anexo n° 04)

a. Identificación de activos de TI

En este punto se identificarán los activos que dan soporte a los procesos de Créditos y Captaciones. Para ello se utilizará la clasificación propuesta por la ISO 27005:2008. Se podrá clasificar los activos de TI, según sus características, en los siguientes tipos:

- Dato: información que se genera, envía, recibe y gestionan dentro de la organización. Incluye los documentos que se gestionan dentro de sus procesos.
- Aplicación: software que se utilice como soporte en los procesos.

- Personal: actores que tienen posibilidades de acceso y manejo, de una u otra manera, de los activos de información.
- Servicio: servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.
- Tecnología: hardware donde se procesa, almacena o transmite la información.
- Instalación: lugar donde se alojan los activos de información. Puede estar ubicado dentro de la entidad o fuera de ella.
- Equipamiento auxiliar: activos que no se hallan definidos en ninguno de los anteriores tipos.

Para obtener el inventario de activos de TI que se van a considerar en la evaluación de riesgos se debe analizar las entradas e insumos requeridos en la ficha técnica. Se podrá aplicar utilizar cualquiera de los dos enfoques que se indican a continuación, independiente o conjuntamente:

- Enfoque top-down (de arriba abajo), infiriendo los activos de información relacionados con los procesos críticos (créditos y captaciones) a partir de la descripción de los procesos.
- Enfoque bottom-up (de abajo arriba), identificando las principales aplicaciones, archivos, bases de datos, equipos, instalaciones, usuarios, etc. utilizados en los procesos.

Para la clasificación de los activos de TI se utilizará el siguiente formato y se tomará como referencia la catalogación de activos del Anexo N° 3:

Tabla N° 03: Plantilla para el registro de los activos de TI por tipo de activo

N°	Tipo de activo de TI	Activo de TI
1		
2		
3		

b. Definición de la criticidad de los activos de TI identificados

Una vez inventariados los activos de TI es necesario identificar y documentar el valor que su seguridad representa para la entidad. Para ello, se asignará un conjunto de valores a cada activo teniendo en cuenta los diferentes requerimientos de seguridad que se consideren relevantes.

El valor que tienen los activos de información para una entidad financiera en el ámbito de la seguridad puede medirse desde diversos puntos de vista. Estos puntos de vista se denominan, en el marco de este modelo, requerimientos de seguridad o dimensiones de la seguridad, los cuales están definidos en el Anexo N° 04.

La valoración se deberá realizar mediante la ponderación de las pérdidas ocasionadas para la entidad financiera en caso de que falle o caiga el activo, debido a la materialización de una amenaza, de cada uno de los requerimientos de seguridad definidos para los diferentes activos de información, según las tablas de

referencia del Anexo N° 04 en relación a: disponibilidad, integridad y confidencialidad.

Las escalas y criterios que se utilizarán para calificar cada una de las dimensiones de seguridad de TI de cada activo, se muestran en la tabla N° 04.

Tabla N° 04: Valores y criterios de referencia para la valoración de la criticidad de los activos de TI

	Valor	Criterio
Disponibilidad	1	**No aplica/No es relevante**
	2	**Debe estar disponible al menos el 10% del tiempo**
	3	**Debe estar disponible al menos el 50% del tiempo**
	4	**Debe estar disponible al menos el 75% del tiempo**
	5	**Debe estar disponible al menos el 95% del tiempo**

	Valor	Criterio
Integridad	1	**No aplica / No es relevante**
	2	**No es relevante los errores que tenga o la información que falte**
	3	**Tiene que estar correcto y completo al menos en un 50%**
	4	**Tiene que estar correcto y completo al menos en un 70%**
	5	**Tiene que estar correcto y completo al menos en un 95%**

	Valor	Criterio
Confidencialidad	1	**No aplica / No es relevante**
	2	**Daños muy bajos, el incidente no trascendería del área afectada**
	3	**Daños bajos, el incidente no trascendería del área afectada**
	4	**Los daños serían relevantes, el incidente implicaría a otras áreas**
	5	**Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas**

Para la valoración de la criticidad de los activos de TI se utilizará el siguiente formato:

Tabla N° 05: Plantilla para la calificación de la criticidad de los activos de TI

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		Confidencialidad	Integridad	Disponibilidad		
1						
2						
3						

Los niveles de criticidad de los activos de TI se obtendrán del producto de las calificaciones realizadas para cada criterio de seguridad y se clasificarán de la siguiente manera:

Tabla N° 06: Niveles de valoración de la criticidad de los activos de TI

Rango	Nivel de criticidad	Descripción
1 – 5	**1**	**Muy bajo**
6 – 10	**2**	**Bajo**
11 – 15	**3**	**Medio**
16 – 20	**4**	**Alto**
21 – 25	**5**	**Muy alto**

B. Identificación de amenazas por activo

En esta actividad caracteriza el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cuán probable es que pase. Es decir, describe las amenazas a los que el sistema está expuesto.

Para la identificación de las amenazas significativas de cada activo de TI identificado, se tomará en consideración lo siguiente:

- El tipo de activo
- Las dimensiones de seguridad con las que cada activo está relacionado
- La experiencia de la organización
- Los reportes de incidentes de seguridad

Tabla N° 07: Ficha técnica de la actividad Identificación de amenazas por activo

Tarea: Identificación de amenazas		
Objetivo Identificar las amenazas relevantes sobre cada activo de TI		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Modelo de valor: Informe del valor de los activos - Informes relativos las vulnerabilidades de la organización - Reportes de incidentes de seguridad de TI	- Relaciones de amenazas significativas por activo	- Entrevistas con los propietarios de los activos - Reuniones con los responsables del uso y mantenimiento de los activos tomarán en cuenta en la valoración de los activos de TI - Utilizar Tabla de Inventario de las amenazas por activo y dimensión de seguridad de la información (ver Anexo N° 05)

Tomando como referencia la tabla de inventario de las amenazas por activo y dimensión de seguridad de la información del Anexo N° 05 y el informe de valor de los activos de la actividad anterior, se debe obtener la relación de amenazas por cada activo de TI. Se utilizará el siguiente formato:

Tabla N° 08: Plantilla para la identificación de amenazas por activo

N°	Activo	Amenaza
1		
2		
3		

C. Identificación de vulnerabilidades por activo

En esta actividad se realiza el análisis de las deficiencias, debilidades y carencias que tiene la organización en los diferentes procesos de TI relacionados a la protección de los activos que han sido identificados. El resultado de esta actividad permitirá determinar cuáles son las debilidades internas que pueden ser aprovechadas por las amenazas para materializarse y hacer fallar o atacar a los activos de TI.

Tabla N° 09: Ficha técnica de la actividad Identificación de vulnerabilidades por activo

Tarea: Identificación de vulnerabilidades por activo		
Objetivo Identificar las vulnerabilidades relevantes sobre cada activo de TI		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Modelo de valor: Informe del valor de los activos - Informes y registro de incidentes de seguridad de la información	- Relaciones de vulnerabilidades posibles por activo	- Entrevistas con los propietarios de los activos - Reuniones con los responsables del uso y mantenimiento de los activos tomarán en cuenta en la valoración de los activos de TI - Utilizar el Listado de vulnerabilidades potenciales (ver Anexo N° 06)

Tomando como referencia el Listado de las vulnerabilidades del Anexo N° 06 y adecuándolo a cada relación activo - amenaza, se identificarán las vulnerabilidades por activo, utilizando el siguiente formato:

Tabla N° 10: Plantilla para la identificación de las vulnerabilidades por cada Activo-Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Activo 1	Amenaza 1.1	Vulnerabilidad 1.1.1
			Vulnerabilidad 1.1.2
		Amenaza 1.2	Vulnerabilidad 1.2.1
			Vulnerabilidad 1.2.2
2	Activo 2	Amenaza 2.1	Vulnerabilidad 2.1.1
			Vulnerabilidad 2.1.2
		Amenaza 2.2	Vulnerabilidad 2.2.1
			Vulnerabilidad 2.2.2
			Vulnerabilidad 2.2.3

D. Valorización del impacto y la probabilidad de ocurrencia de las amenazas

Esta actividad permitirá valorizar la materialización de cada una de las amenazas identificadas para cada activo de TI, tomando como referencia las vulnerabilidades encontradas para cada una de ellas. La valorización de las amenazas se realizará en base a la calificación de sus dos insumos principales, como son: el impacto que pueden ocasionar y la probabilidad de su ocurrencia.

Para la realización de dicha valorización, el estándar ISO 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. En la propuesta, se optó 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.

Tabla N° 11: Ficha técnica de la actividad Estimación del impacto y la probabilidad de ocurrencia de las amenazas

Tarea: Estimación del impacto y la probabilidad de ocurrencia de las amenazas		
Objetivos - Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo - Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Listado de amenazas identificadas por activo de TI - Informes de vulnerabilidades - Historia o antecedentes de incidentes de seguridad de TI	- Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos	- Entrevistas con los propietarios de los activos - Reuniones con los responsables del uso y mantenimiento de los activos tomarán en cuenta en la valoración de los activos de TI - Valoración Delphi

a. Estimación del impacto de una amenaza

Para la estimación del impacto de cada una de las amenazas identificadas se utilizará la siguiente tabla que define los niveles de impacto de las amenazas:

Tabla N° 12: Valoración de los niveles de impacto de una amenaza

Nivel	Impacto	Descripción
1	Insignificante	Tiene un efecto nulo o muy pequeño en las operaciones de créditos y captaciones
2	Menor	Afecta parcialmente las operaciones de créditos y captaciones. Paraliza servicios que no afectan directamente al cliente.
3	Moderado	Operativamente es sostenible, pero dificulta o retrasa las operaciones de créditos y captaciones. Paraliza parcialmente los servicios críticos a clientes
4	Mayor	Paraliza la atención de servicios críticos a clientes, debido a la caída significativa de las operaciones de créditos y captaciones Pérdida potencial de clientes
5	Catastrófico	Paraliza todas las operaciones de créditos y captaciones de la entidad

b. Estimación de la probabilidad de ocurrencia de una amenaza
Para la estimación de la probabilidad de ocurrencia de cada una de las amenazas consideradas se utilizará la siguiente tabla que define los niveles de probabilidad de ocurrencia o frecuencia de las amenazas:

Tabla N° 13: Valoración de los niveles de probabilidad de ocurrencia de una amenaza

Nivel	Probabilidad	Descripción
1	**Raro**	**No se registra en los últimos 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**

1.4.11.2. Fase 2: Clasificación del riesgo de TI

a. Determinación del apetito y la tolerancia al riesgo
Para determinar el apetito y la tolerancia al riesgo en el modelo propuesto, se debe entender que éste está enmarcado dentro del Riesgo Operacional, entendiéndose éste, como un incidente que ocasiona que el resultado de un proceso de negocio difiera del resultado esperado, debido a fallas en los procesos internos, las personas, los sistemas o por eventos externos. El riesgo operacional incluye el riesgo tecnológico y excluye el riesgo estratégico. Por tanto, para determinar el apetito y la tolerancia al riesgo de TI solo se contemplará las que provienen del Riesgo Operacional Tecnológico, es decir de las fallas de los sistemas tecnológicos.

Dado que los riesgos operacionales se originan por debilidades del control, es decir por las deficiencias en los controles que muestran que los riesgos operacionales no se encuentran identificados y/o no se encuentran adecuadamente mitigados, lo que conllevaría a no lograr un objetivo del negocio y/o producir una pérdida financiera.

Los posibles escenarios de riesgo de TI que se tomarán en cuenta para la clasificación se muestran en la siguiente tabla.

Tabla N° 14. Catálogo de posibles escenarios de riesgo de TI

Ámbito del escenario de riesgo de TI	Escenario de riesgo de TI
Infraestructura física de TI	Obsolescencia
	Daño o destrucción
	Robo
	Inadecuada arquitectura
	Instalación y cambios
Relacionados con el personal de TI	Ausencia del personal
	Falta de habilidades y experiencia del personal
	Insuficiencia de personal especializado
Gestión de proyectos	Proyectos no finalizados
	Riesgos económicos del proyecto
	Retraso en entrega de proyectos
	Baja calidad en los proyectos
	Falta de visión de programa de proyectos
Gestión de la seguridad	Ataque lógico a la seguridad
	Traspasar la seguridad
	Alteración de la integridad de la información

	Exposición de la información
Aplicaciones	Incorrectas decisiones de inversión en aplicaciones
	Envejecimiento de las aplicaciones de negocio
	Implementación inadecuada de las aplicaciones
	Inestabilidad de las aplicaciones
	Falta de capacidad de las aplicaciones
	Envejecimiento de las aplicaciones de infraestructura
	Aplicaciones intrusas
Entrega y soporte de servicios de TI	Entrega y soporte de servicios
	Rendimiento de los servicios
Cumplimiento legal	Cumplimiento legal
Otros escenarios	Rendición de cuentas de TI
	Integración de TI y los procesos de Negocio
	Errores operativos de TI
	Procesos operativos de TI

Para clasificar los niveles de riesgo de TI se utilizará la siguiente escala de 5 puntos:

a. Muy Bajo: cuando la deficiencia del control no impide el logro de un objetivo y no representa exposición a una pérdida significativa para las Microfinancieras de Chiclayo. Es irrelevante. Se califica con este nivel para los escenarios siguientes:

Obligaciones legales	Pudiera causar el incumplimiento leve o técnico de una ley o regulación
Seguridad	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
Intereses comerciales y económicos	supondría pérdidas económicas mínimas
Interrupción del servicio	Pudiera causar la interrupción de actividades propias de las Microfinancieras de Chiclayo
Operaciones	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
Administración y gestión	pudiera impedir la operación efectiva de una parte de las Microfinancieras de Chiclayo
Pérdida de confianza (reputación)	no supondría daño a la reputación o buena imagen de las personas u organizaciones
Persecución de delitos	Dificulte la investigación o facilite la comisión de delitos
Tiempo de recuperación del servicio	3 días < RTO

b. Bajo: cuando la deficiencia del control genera daños menores a las Microfinancieras de Chiclayo, es decir genera pérdidas pero no significativas. Se califica con este nivel para los escenarios siguientes:

Obligaciones legales	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
Seguridad	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
Intereses comerciales y económicos	de bajo interés para la competencia de bajo valor comercial
Interrupción del servicio	Probablemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo
Operaciones	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
Administración y gestión	probablemente impediría la operación efectiva de una parte de las Microfinancieras de Chiclayo

Pérdida de confianza (reputación)	Probablemente afecte negativamente a las relaciones internas de la Organización
Persecución de delitos	Dificulte la investigación o facilite la comisión de delitos
Tiempo de recuperación del servicio	1 día < RTO < 5 días

c. Medio: cuando la deficiencia del control podría resultar en una pérdida significativa o importante, pero dentro de rangos aceptables para las Microfinancieras de Chiclayo. Se califica con este nivel para los escenarios siguientes:

Obligaciones legales	probablemente sea causa de incumplimiento de una ley o regulación
Seguridad	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
Intereses comerciales y económicos	de cierto interés para la competencia causa de pérdidas financieras o merma de ingresos
Interrupción del servicio	Probablemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo con impacto en otras organizaciones o en los clientes
Operaciones	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
Administración y gestión	probablemente impediría la operación efectiva de más de una parte de la Organización
Pérdida de confianza (reputación)	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
Persecución de delitos	Dificulte la investigación o facilite la comisión de delitos
Tiempo de recuperación del servicio	3 horas < RTO < 1 día

d. Alto: cuando la deficiencia del control podría resultar en una pérdida significativa, del tipo económico u operativo.

Obligaciones legales	probablemente cause un incumplimiento grave de una ley o regulación
Seguridad	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
Intereses comerciales y económicos	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas
Interrupción del servicio	Probablemente cause una interrupción seria de las actividades propias de las Microfinancieras de Chiclayo con un impacto significativo en otras organizaciones
Operaciones	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
Administración y gestión	probablemente impediría la operación efectiva de las Microfinancieras de Chiclayo
Pérdida de confianza (reputación)	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
Persecución de delitos	Impida la investigación de delitos graves o facilite su comisión
Tiempo de recuperación del servicio	1 hora < RTO < 3 horas

e. Muy Alto: cuando la deficiencia del control expone a las Microfinancieras de Chiclayo a una pérdida sustancial material, económica y/o sanción regulatoria, no aceptable para las Microfinancieras de Chiclayo.

Obligaciones legales	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
Seguridad	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
Intereses comerciales y económicos	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas
Interrupción del servicio	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
Operaciones	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
Administración y gestión	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
Pérdida de confianza (reputación)	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
Persecución de delitos	Impida la investigación de delitos graves o facilite su comisión
Tiempo de recuperación del servicio	RTO < 1 hora

Para determinar el apetito y la tolerancia en cada uno de los escenarios de riesgos de TI definidos que podrían afectar el no cumplimiento de los objetivos estratégicos u operacionales, se utilizará la siguiente estructura:

Tabla N° 15. Plantilla para determinar el apetito y la tolerancia al riesgo de TI por cada objetivo estratégico u operacional

Objetivo Estratégico u Operacional de las Microfinancieras de Chiclayo		
Apetito de riesgo		
Tolerancia de riesgo		
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI		
Relacionados con el personal de TI		
Gestión de proyectos		
Gestión de la seguridad		
Entrega y soporte de servicios de TI		
Cumplimiento corporativo		
Cumplimiento legal		
Otros escenarios		

b. Cálculo de los niveles de riesgos intrínseco (NRI)
El cálculo del nivel de riesgos intrínseco de cada una de las amenazas identificadas para cada activo, estará en función de la valoración y clasificación del impacto y la probabilidad de su ocurrencia. Se utilizará la siguiente relación:

NRI = Probabilidad de ocurrencia x Impacto

El producto de esta relación se ubicará en el siguiente mapa de calor (ver tabla 15), tomando como referencia los niveles de riesgo definidos anteriormente.

Tabla N° 16: Matriz de calor para la valoración del impacto y probabilidad de las amenazas

Impacto en los procesos	Probabilidad de ocurrencia				
	Raro	Improbable	Posible	Probable	Casi seguro
Catastrófico	Bajo	Medio	Alto	Muy alto	Muy alto
Mayor	Bajo	Bajo	Medio	Alto	Muy alto
Moderado	Muy bajo	Bajo	Medio	Medio	Alto
Mínimo	Muy bajo	Bajo	Bajo	Bajo	Medio
Insignificante	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

1.4.11.3. Fase 3: implementación de controles

En esta fase se definirá e implementará los controles o salvaguardas necesarias para tratar cada una de las amenazas en cuya evaluación se haya obtenido niveles de riesgos no tolerantes, es decir, con el calificativo de “Alto” o “Muy Alto”.

Esta fase contempla las siguientes actividades y tareas:
a. Plan de tratamiento de los riesgos intrínsecos
b. Implementación de las medidas de seguridad
c. Identificación de la estrategia de implementación de controles
d. Evaluación de la brecha de seguridad: nivel de riesgo residual (NRR)

a. Plan de tratamiento de los riesgos intrínsecos

Luego de definir los niveles de riesgos intrínsecos para cada una de las vulnerabilidades de cada amenaza de cada activo que puedan afectar su integridad, confidencialidad o disponibilidad; se debe definir el criterio de aceptación del riesgo, el cual determina si el riesgo es aceptable o si requiere de algún tratamiento. Esto se determina con el Apetito del Riesgo de TI definido anteriormente.

Los NRI cuya valoración sea “Muy Alta” o “Alta” son los que se tratarán mediante controles o salvaguardas para reducir la probabilidad que dichos riesgos identificados se materialicen o para reducir su impacto. Para las amenazas con NRI “Medio”, “Baja” o “Muy Baja” se aplicará la estrategia de convivir con el riesgo.

A continuación se presenta los criterios de aceptación o no aceptación para dada uno de los niveles de los riesgos intrínsecos:

Tabla N° 17: Apetito al riesgo de TI según el nivel de exposición al riesgo

Nivel de Riesgo	Política para la toma de Acciones
Muy alto	**Riesgo no aceptable**
Alto	**Riesgo no aceptable**
Medio	**Riesgo aceptable**
Bajo	**Riesgo aceptable**
Muy bajo	**Riesgo aceptable**

Luego, se determina el plan de tratamiento para cada uno de los riesgos encontrados no aceptables.

b. Implementación de las medidas de seguridad

Los controles que se seleccionarán para el tratamiento de los riesgos no aceptables, se obtendrán del Anexo N° 07 y que pertenecen al estándar ISO 17799 (ISO/IEC 27002), el cual contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general.

Para determinar los controles que se van a implementar se desarrollará la Declaración de la Aplicabilidad, donde se mostrarán los controles que se implementarán, adaptados a la realidad organizacional y capacidad instalada de Las Microfinancieras de Chiclayo.

Para empezar, se deberá definir las políticas de seguridad que Las Microfinancieras de Chiclayo deberá declarar o mejorar para alcanzar el nivel de seguridad de la información deseado. Éstos deberán ser desarrollados y promovidos por la Dirección de Las Microfinancieras de Chiclayo.

c. Identificación de la estrategia de implementación de controles

Seleccionado el control, con su correspondiente objetivo de control, para cada NRI no aceptable, se debe definir la estrategia de implementación del control, que puede ser:

- Aceptar el riesgo
- Elección de controles para mitigar los riesgos
- Transferencia del riesgo a terceros
- Evitar aumento del riesgo

d. Cálculo Nivel de Riesgo Residual (NRR) para determinar la brecha de seguridad

El cálculo del Nivel de Riesgo Residual (NRR) se realizará luego de implementado el control y de la evaluación de su efectividad y cumplimiento, obteniendo luego la brecha de seguridad con respecto al Nivel de Riesgo Intrínseco.

II. MARCO TEÓRICO

2.1. ANTECEDENTES

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.

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 chiclayo, 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.

2.2. BASES TEÓRICO

2.2.1. La Superintendencia de Banca, Seguros y AFPs (SBS)

La Superintendencia de Banca, Seguros y AFP es el organismo encargado de la regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SPP.

La SBS es una institución de derecho público cuya autonomía funcional está reconocida por la Constitución Política del Perú. Sus objetivos, funciones y atribuciones están establecidos en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP (Ley 26702).

2.2.2. Definición de Riesgo de TI

De acuerdo a ISACA (2009) en los Lineamientos para la Gestión de Seguridad de TI publicadas por la Organización Internacional de Estandarización (ISO) en su (ISO/IEC PDTR 13335−1), riesgo es el potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y, por consiguiente, ocasione pérdida o daño a la organización.

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

Amenazas: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza

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

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).

2.2.2.1. Gestión de Riesgo

Costas Santos (2011) establece que la Gestión de los Riesgos permite tener control sobre el desarrollo, la implementación y funcionamiento de los procesos, lo cual llevara a lograr de manera eficiente el cumplimiento de sus objetivos estratégicos y estar preparados para enfrentar cualquier incidente que pueda presentarse.

Sobre los procesos, se construyen controles con el objetivo de reducir la frecuencia de las amenazas o limitar el daño causado y llevar el nivel de riesgo a un nivel aceptable por la organización.

Dependiendo del tipo de riesgo, se puede optar por:

- Evitar el riesgo: por ejemplo eliminando el activo.
- Mitigar el riesgo: implementando controles para reducir la probabilidad y el impacto.
- Transferir el riesgo: por ejemplo contratando un seguro con cobertura para ese riesgo.
- Aceptar el riesgo: reconociendo que el riesgo existe y monitorizarlo.

Una vez que los controles han sido aplicados, el nivel de riesgo que queda es el riesgo residual. Como se establece en los Requerimientos de los Sistemas de Gestión de Seguridad de la Información en la norma ISO 27001; la Dirección debe establecer el nivel de riesgo aceptable para la organización. Los riesgos que excedan de ese nivel deben ser reducidos.

2.2.2.2. Nivel de Riesgo Aceptable

De acuerdo a Costas Santos (2011), riesgo aceptable es el que conlleva un potencial de perdida menor y que de producirse fallas operacionales no afectan significativamente las condiciones de la operación. […] los activos con riesgo extremo e intolerable deben ser llevados al menos al nivel tolerable. Y en el caso de activos críticos deben ser llevados al nivel aceptable.

Para la aceptación definitiva de los riesgos se debe tener en cuenta:

- La Política organizacional.
- Sensibilidad y criticidad de los activos involucrados.
- Niveles aceptables de los posibles impactos.
- Rentabilidad de la implementación.

2.2.3. Normas ISO relacionadas con la Gestión de Riesgos de TI

Las Normas ISO, ofrecen una visión ordenada y metodológica para implantar un programa de seguridad de la información, de forma tal de tener una guía que contemple todos los aspectos sobre el tema y que es producto de los representantes internacionales con mayores fortalezas en la disciplina.

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los principios de confidencialidad, integridad y disponibilidad de la información. Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación. Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información.

El ISO 27001:2005, establece un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme con el objetivo de hacer sostenibles en el tiempo todas las iniciativas en materia de seguridad de la información.

Todas las metodologías y estándares que respalden la gestión de riesgos de TI/SI, se aplican eficientemente si se ejecutan sus herramientas de manera automatizada, pero en la actualidad en nuestro mercado no existen o son pocos aplicables por sus costos elevados.

2.2.4. Norma ISO/IEC 27001

Hoy por hoy el mundo de la seguridad se debate en dos posturas de instituciones muy respetables, las cuales han regido el mundo de las normas internacionales en por muchos años, cada uno en diferentes lugares del mundo; y cada uno con una aproximación diferente. Por una parte tenemos a ISO y por otra parte tenemos a NIST cada una de estas instituciones ha propuesto un marco de trabajo para el tema se la seguridad informática.

Lo primero que debemos aclarar es la procedencia de las dos organizaciones la ISO es bien conocida en el mundo como la organización que se encarga de fijar las normas aceptadas en Europa y en buena parte del mundo. Por su parte en USA, su contraparte en la materia es el NIST. Cada una tiene una postura frente al manejo de la seguridad informática que a lo largo de este artículo daremos a conocer para que el lector pueda tener una opinión informada al respecto.

Ante la necesidad de fijar un estándar en la industria la ISO adapto el estándar ingles que había sido promulgado con anterioridad el BS7799, que había tomado una gran fuerza como documento base en seguridad informática, documento el que poseía en su momento la versiones 7799-1 código de prácticas para la administración de seguridad en

informática. Este documento es una guía general para encargados de seguridad en corporaciones Cuando fue publicado el estándar vigente a diciembre del 2001 servía como guía de implementación, pero no explica particularidades de los sistemas ni su implementación particular.

Según ISACA (2009), esta norma muestra cómo aplicar los controles propuestos en la ISO 17799, estableciendo los requisitos para construir un SGSI, "auditable" y "certificable", respecto a los controles, aparecen como anexos. Estos más los que la organización desee incorporar, deberán conformar un sólido sistema que permita el fin último: la seguridad de la información.

El SGSI de la ISO 27001 le permite prevenir o reducir eficazmente el nivel de riesgo mediante la implantación de los controles adecuados, preparando la organización ante posibles emergencias, garantizando la continuidad del negocio.

La norma responde a la aplicación del modelo PDCA (Plan-Do-Check-Act) de mejora continua también existente en otras normas. La aplicación del proceso PDCA en el SGSI conforma un modelo de gestión de riesgos que guía la estrategia de “Corporate Governance”, incluyendo la gestión de riesgos de negocios. […] bajo el esquema común del modelo PDCA, la ISO 27001 también ofrece un interesante alineamiento con otras normas también de sistemas de gestión, como la ISO 9001 de Calidad y la ISO 14001 de Medio Ambiente, lo que se traduce en reducción de esfuerzos y costos en una implementación integrada.

Entre los principales beneficios de la implementación de ésta norma se tiene:

- Establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada.
- Reducción de riesgos de pérdida, robo o corrupción de la información.
- Los clientes tienen acceso a la información de manera segura, lo que se traduce en confianza.
- Los riesgos y sus respectivos controles son revisados constantemente.
- Las auditorías externas permiten identificar posibles debilidades del sistema.
- Continuidad en las operaciones del negocio tras incidentes de gravedad.
- Garantizar el cumplimiento de las leyes y regulaciones establecidas en materia de gestión de información.
- Incrementa el nivel de concientización del personal con respecto a los tópicos de seguridad informática.
- Proporciona confianza y reglas claras al personal de la empresa.
- Provee la seguridad como una ventaja competitiva para las empresas que realizan operaciones de comercio electrónico.
- Aporta grandes beneficios para los bancos que requieren reducir riesgos operacionales, introducido por el Nuevo Acuerdo de Capitales Basilea II.
- Es consistente con lo establecido en regulaciones como la Ley Sarbanes-Oxley.

2.2.5. Norma ISO/IEC 17799

Tiene su origen en la norma BS7799-2 donde se detallan las especificaciones para la administración de seguridad en informática. Es una guía en la implementación de seguridad en organizaciones.

Según ISACA (2009), normativas como ISO/IEC 17799 asisten en la implantación y especialmente en la gerencia de día-a-día para enfrentar la proliferación de comunicación y discontinuidad de tecnología. Es por esta razón que componentes de esquemas como ISO asisten en la realización de seguridad tanto financieras como de red informática.

Una vez implantada la misma propicia mejoras concurrente con los avances en tecnología y proliferación de comunicación. La vulnerabilidad de sistemas es una situación que cambia a diario, no es una situación de semanas o meses, es de días u horas.

Para implantar ISO/IEC 17799 se requiere capacitar al personal no necesariamente y únicamente en aspectos tecnológicos pero en el trabajo de equipo y asegurar un avance del sistema de gerencia concurrente con la realidad tecnológica y comunicación. Esta capacitación incluye bases fundamentales de gerencia contemporánea incluyendo riesgos desde análisis de vulnerabilidad hasta mitigación o "Disaster Recovery".

En una secuencia lógica, los objetivos de cada dominio propuesto en la normativa ISO/IEC 17799 son:

a) Política de la Seguridad
b) Organización de la Seguridad
c) Seguridad del Personal
d) Clasificación y control del activo
e) Control de Acceso del Sistema
f) Seguridad física y ambiental
g) Desarrollo y Mantenimiento del Sistema
h) Administración del Procesador y de la Red (Conectividad)
i) Hojas de operación (planning) de la Continuidad del Negocio
j) Conformidad

2.2.6. Metodología de Gestión de Riesgo de TI

Una metodología de gestión de riesgos consiste en cómo debe llevarse a cabo para cumplir con lo establecido por la Norma ISO 27001. En un contexto general debe estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización y posteriormente implementar el o los controles adecuados para su tratamiento.

Según ISACA (2009), las etapas mínimas que debe contemplar una metodología de gestión de riesgos de TI son:

2.2.6.1. Estimación de Riesgos

La estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos:

- La identificación de riesgos, genera una lista de riesgos capaces de afectar el funcionamiento normal del entorno informático.
- El análisis de riesgos, mide su probabilidad de ocurrencia y su impacto en la organización.
- La asignación de prioridades a los riesgos.

2.2.6.2. Identificación de Riesgos

En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático. Los principales factores que se ven afectados son:

- Creación de la planificación; Incluye la planificación excesivamente optimista, planificación con tareas innecesarias, y organización de un entorno informático sin tener en cuenta áreas desconocidas y la envergadura del mismo.

- La organización y gestión; presupuestos bajos, el ciclo de revisión/decisión de las directivas es más lento de lo esperado.

- El entorno de trabajo; mal funcionamiento de las: herramientas de desarrollo, espacios de trabajo inadecuados y la curva de aprendizaje de las nuevas tecnologías es más larga de lo esperado.

- Las decisiones de los usuarios finales; falta de participación de los usuarios finales y la falta de comunicación entre los usuarios y el departamento de informática

- El personal contratado; Falta de motivación, falta de trabajo en equipo y trabajos de poca calidad.

- Los procesos, que incluye: La burocracia, falta de control de calidad y la falta de entusiasmo.

Se puede considerar como los orígenes de la Administración de los Riesgos de TI a los siguientes aspectos:

- Requerimientos legales, regulatorios, contractuales
- Acelerados avances tecnológicos
- Incidentes de seguridad (comunicaciones divulgadas)
- Preocupación de los usuarios
- Pérdidas económicas
- Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

2.2.6.3. Análisis de Riesgos

Una vez hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución. La explicación de Análisis de riesgos se extenderá posteriormente.

2.2.6.4. Exposición a Riesgos

Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.

2.2.6.5. Estimación de la Probabilidad de Pérdida

Las principales formas de estimar la probabilidad de pérdida son las siguientes:

- Disponer de la persona que está más familiarizada con el entorno informático para que estime la probabilidad de ocurrencia de eventos perjudiciales.
- Usar técnicas Delphi o de consenso en grupo. El método Delphi consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos del riesgo.
- Utilizar la calibración mediante adjetivos, en la cual las personas involucradas eligen un nivel de riesgo entre (probable, muy probable) y después se convierten a estimaciones cuantitativas.

2.2.6.6. Priorización de Riesgos

En este paso de la estimación de riesgos, se estiman su prioridad de forma que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico se puede dejar en un segundo plano.

2.2.6.7. Control o tratamiento de Riesgos

Una vez que se hayan identificado los riesgos del entorno informático y analizado su probabilidad de ocurrencia, existen bases para controlarlos que son:

- Planificación
- Resolución de riesgos
- Monitorización de riesgos

2.2.6.8. Planificación de Riesgos

Su objetivo, es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestas las actividades informáticas.

2.2.6.9. Resolución de Riesgos (Incluye Mitigación y transferencia de riesgos)

La resolución de los riesgos está conformada por los métodos que controlan el problema de un diseño de controles inadecuado, los principales son:

- Evitar el Riesgo: No realizar actividades arriesgadas.
- Conseguir información acerca del riesgo.
- Planificar el entorno informático de forma que si ocurre un riesgo, las actividades informáticas sean cumplidas.
- Eliminar el origen del riesgo, si es posible desde su inicio.
- Asumir y comunicar el riesgo.

2.2.6.10. Monitorización de Riesgos

Consiste en verificar el desempeño del sistema de gestión de riesgo y los cambios que pudieran afectarlo.

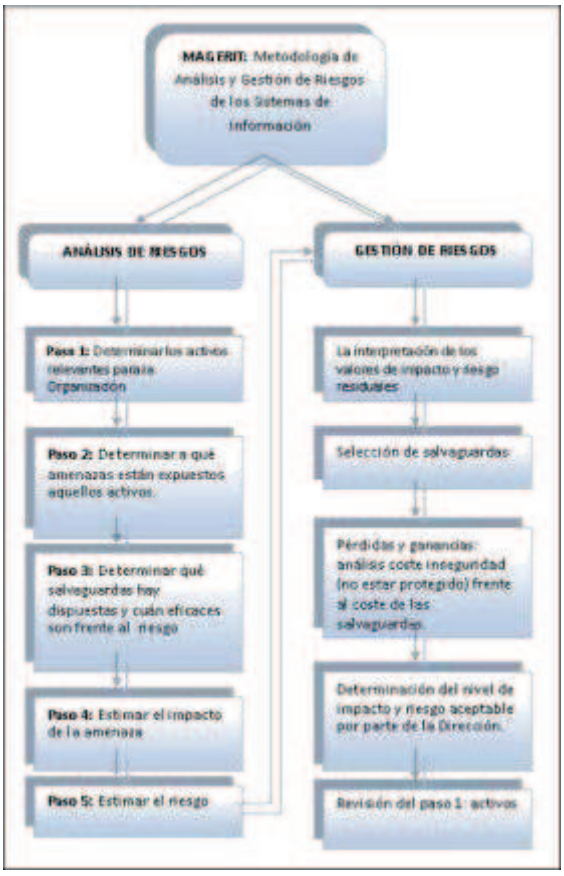
2.2.7. Metodología MAGERIT

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.

Gráfico N° 03: Elementos del proceso de análisis y gestión de riesgos



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.

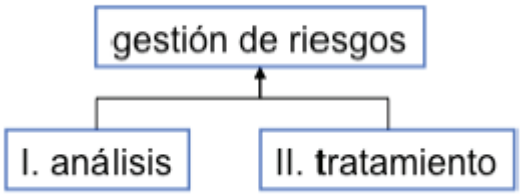
La gestión de riesgos, permite organizar la defensa de manera concienzuda y prudente, posibilitando defensas para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

MAGERIT considera dos grandes tareas a realizar:

1. análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.
2. tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo 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.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos.

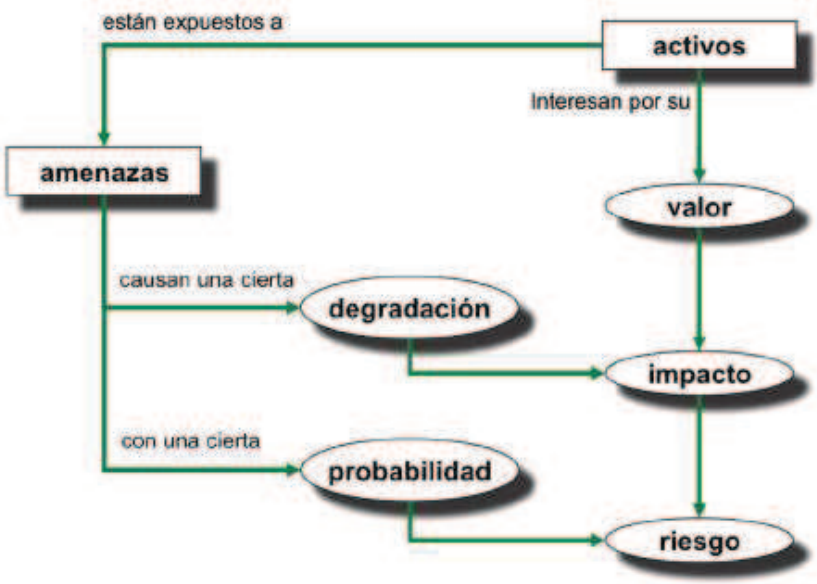
Gráfico N° 04: Etapas ara la Gestión de Riesgos según MAGERIT



Para el análisis de riesgos MAGERIT propone los pasos siguientes:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Gráfico N° 05: Elementos del análisis de riesgos potenciales según MAGERIT



2.2.8. Apetito y tolerancia al riesgo

El apetito es el nivel de riesgo que la empresa quiere aceptar, aquél con el que se siente cómoda, su tolerancia será la desviación respecto a este nivel. Por otro lado, la capacidad de asumir riesgos, será el nivel máximo de riesgo que una organización puede soportar en la persecución de sus objetivos. Así, la tolerancia servirá como alerta para evitar que la empresa llegue al nivel establecido por su capacidad, algo que pondría en peligro la continuidad del negocio (Instituto de auditores internos de España, 2012)

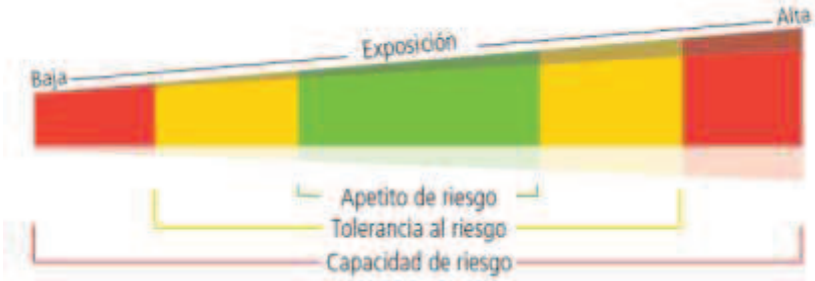
En ese sentido, podemos definir lo siguiente:

a. El apetito de riesgo: La cantidad de riesgo que una organización está dispuesta a buscar o aceptar en la búsqueda de sus objetivos a largo plazo.

b. Tolerancia al riesgo: Los límites de la asunción de riesgos, fuera de la cual la organización no está dispuesta a aventurarse en la búsqueda de sus objetivos a largo plazo.

c. Capacidad de riesgo: la capacidad de llevar los riesgos, y la madurez de gestión de riesgos para su gestión.

Gráfico N° 06: Determinación del apetito y la tolerancia al riesgo



2.2.9. Indicadores de riesgos clave (KRI)

Un indicador de riesgos clave (KRI) es una métrica para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo de la organización (es decir, el nivel de riesgo que la compañía está preparada para aceptar), y tenga un impacto profundamente negativo en la capacidad de tener éxito de una organización.

Si una organización se especializa en ventas al por menor, por ejemplo, un indicador de riesgo clave podría ser el número de quejas de los clientes, porque el aumento de este KRI podría ser una indicación temprana de que hay que resolver un problema operativo.

El desafío para una organización no es solo identificar cuáles indicadores de riesgo deben ser identificados como claves (los más importantes), sino también comunicar esa información de tal manera que todo el mundo en la organización entienda claramente su significado.

Identificar indicadores de riesgos clave requiere la comprensión de las metas de la organización.

Cada KRI debería ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización (KPI). Los indicadores de rendimiento clave, que a menudo se confunden con los indicadores de riesgos clave, son las métricas que ayudan a una organización a evaluar el progreso hacia los objetivos declarados.

III. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS DE O LOS INSTRUMENTO UTILIZADOS

3.1 IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE TI DE LOS PROCESOS PRINCIPALES DE LAS MICICROFINANCIERAS DE CHICLAYO

Aplicando el enfoque bottom-up (de abajo arriba), se ha identificado los siguientes activos de TI que le dan soporte a los procesos de las microfinancieras:

Tabla N° 18: Inventario de activos de TI de los procesos de las microfinancieras

N°	ACTIVO
1	Servidor principal de dominio (DNS)
2	Servidor principal de base de datos y aplicaciones
3	Red de comunicaciones
4	Sala de servidores del Centro de Procesamiento Central y del Centro de Procesamiento Alterno
5	Bases de Datos
6	Backups de base de datos
7	Personal de área de TI
8	Aplicaciones informáticas de créditos y captaciones Incluye: Sistema de Información Financiera (SIIF)
9	Correo electrónico institucional
10	Equipos de cómputo terminales de ventanilla y analistas de créditos:
11	Código fuente de las aplicaciones Incluye: biblioteca de versiones, librerías
12	Archivos de Actas de conformidad
13	Archivo de requerimientos informáticos (físico)
14	Analistas de sistemas (Responsables de la implementación de requerimientos)
15	Equipos de cómputo del Área de Desarrollo
16	Backups o respaldos de desarrollo y mantenimiento
17	Herramientas de desarrollo

Utilizando la clasificación propuesta por la ISO 27005:2008, se tiene el siguiente resultado:

Tabla N° 19: Clasificación de los activos de TI identificados

N°	Tipo de activo	Activo
1	Aplicaciones	Aplicaciones informáticas de créditos y captaciones
2	Aplicaciones	Herramientas de desarrollo
3	Comunicaciones	Red de comunicaciones
4	Datos o documentos	Código fuente de las aplicaciones
5	Datos o documentos	Archivos de Actas de conformidad
6	Datos o documentos	Archivo de requerimientos informáticos (físico)
7	Datos o documentos	Registros de control de cambios de las aplicaciones
8	Equipos informáticos	Equipos de cómputo terminales de ventanilla y analistas de créditos
9	Equipos informáticos	Equipos de cómputo del Área de Desarrollo
10	Información	Bases de Datos
11	Información	Backups de documentos normativos y de gestión
12	Instalaciones	Sala de servidores o Centro de Procesamiento Central
13	Personal	Personal de área de TI
14	Personal	Analistas de sistemas (Responsables de la implementación de requerimientos)
15	Servicios	Servidor principal de dominio
16	Servicios	Servidor principal de base de datos y aplicaciones
17	Servicios	Correo electrónico institucional

3.2. DEFINICIÓN DE LA CRITICIDAD DE LOS ACTIVOS DE TI IDENTIFICADOS

Una vez inventariados los activos de TI se ha valorado y clasificado su nivel de importancia o criticidad, tomando como base la calificación dada a cada característica o dimensión de seguridad de la información, de acuerdo a las escalas de valoración propuestas, obteniéndose los siguientes resultados (usando el formato de la tabla N° 05):

Tabla N° 20: Valoración del nivel de criticidad de los activos de TI identificados

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		C	I	D		
1	**Servidor principal de dominio**	**4**	**5**	**5**	**4**	**Alto**
2	**Servidor principal de base de datos y aplicaciones**	**5**	**5**	**5**	**5**	**Muy Alto**
3	**Red de comunicaciones**	**4**	**1**	**5**	**3**	**Medio**
4	**Sala de servidores**	**4**	**1**	**5**	**3**	**Medio**
5	**Bases de Datos**	**5**	**5**	**5**	**5**	**Muy Alto**
6	**Backups de base de datos**	**5**	**5**	**5**	**5**	**Muy Alto**
7	**Personal de área de TI**	**4**	**1**	**5**	**3**	**Medio**
8	**Aplicaciones informáticas de créditos y captaciones**	**4**	**4**	**5**	**4**	**Alto**
9	**Correo electrónico institucional**	**4**	**4**	**5**	**4**	**Alto**
10	**Equipos de cómputo terminales de ventanilla y analistas de créditos:**	**5**	**5**	**5**	**5**	**Muy Alto**
11	**Código fuente de las aplicaciones**	**4**	**5**	**5**	**4**	**Alto**
12	**Archivos de Actas de conformidad**	**2**	**3**	**5**	**3**	**Medio**
13	**Archivo de requerimientos informáticos (físico)**	**2**	**3**	**5**	**3**	**Medio**
14	**Analistas de sistemas**	**4**	**1**	**5**	**3**	**Medio**
15	**Equipos de cómputo del Área de Desarrollo**	**4**	**5**	**5**	**4**	**Alto**
16	**Backups o respaldos de desarrollo y mantenimiento**	**4**	**5**	**5**	**4**	**Alto**

3.3. IDENTIFICACIÓN DE LAS AMENAZAS DE LOS ACTIVOS DE TI

Para cada activo de TI se han identificado las siguientes amenazas (usando el formato de la tabla N° 07):

Tabla N° 21: Listado de amenazas por Activo de TI

N°	Activo	Amenaza
1	Servidor principal de dominio	Paralización de procesos y actividades del negocio, no se accede a los servicios de red
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)
3	Red de comunicaciones	Paralización de servicios de comunicación
4	Sala de servidores	Sabotaje a las instalaciones
		Pérdida de Activos de TI en la sala de servidores (costo de hardware / paralización de Operaciones)
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos
		Falta de espacio de almacenamiento
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos
		Modificación, divulgación y destrucción de la información
8	Aplicaciones informáticas de créditos y captaciones	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente.
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debido errores en la integridad de los datos
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor
10	Equipos de cómputo terminales de ventanilla y analistas de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.
14	Analistas de sistemas (Responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software
15	Equipos de cómputo del Área de Desarrollo	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos
16	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible.

3.4. IDENTIFICACIÓN DE LAS VULNERABILIDADES DE LOS ACTIVOS DE TI

Se han identificado las siguientes vulnerabilidades (usando el formato de la tabla N° 09), el cual es el resultado del análisis de incidentes de seguridad de la información que tienen registrados la microfinancieras de Chiclayo:

Tabla N° 22: Listado de vulnerabilidades por Activo de TI – Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Servidor principal de dominio	Paralización de procesos y actividades del negocio, no se accede a los servicios de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio
			Falla en los componentes físicos
			Fallas en el sistema operativo, falta de actualización de parches
			No se cuenta con un plan de mantenimiento de los servidores
			Ataque de virus
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)	Administrador tiene acceso total a la base de datos y puede realizar modificaciones
			Deficiencia en el diseño de base datos (normalización de BD).
			Usuarios acceden a servidor de base de datos por canales no autorizados
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones
			Falla de la red de comunicaciones con otras agencias
			Fallas eléctricas que generen la interrupción de los procesos y servicios
			No se cuenta con servidor de firewall a nivel de hardware
4	Sala de servidores o Centro de Procesamiento Central	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores.
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.
		Pérdida de Activos de TI en la sala de servidores (costo de hardware / paralización de Operaciones)	No se mantiene un control o registro de acceso a las áreas restringidas
			Falta de un registro de acceso a la sala de servidores
			No se tiene una política y procedimiento para el personal que realiza mantenimiento en la institución
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento). Y revisión de maletines.
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD
			Existencia de passwords no adecuados para usuarios locales y de red
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente
			Acceso a la BD desde otras aplicaciones
			Virus informáticos
			Realización de copias no autorizadas de la Base de Datos.
			Modificación no autorizada de BD
		Falta de espacio de almacenamiento	Incremento de tranSACiones
			No existe un procedimiento de mantenimiento de a BD.
			Incremento de espacio por virus.
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Fallas en los dispositivos de almacenamiento (disco duro del servidor)
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo
			Errores en el proceso de generación de backups
			No se lleva un registro de la generación de backups
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información	Inadecuada segregación de funciones
			No existe un plan de capacitación adecuado

		debido a fuga de talentos	Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos
			Falta de control y seguimiento de accesos
			Falta de acuerdos de confidencialidad
			Impulsos mezquinos que hace que el personal actúe de manera anormal en el desarrollo de sus labores
			Falta de procedimiento de mantenimiento de usuarios
8	Aplicaciones informáticas de créditos y captaciones	Paralización de procesos debido a Problemas en el procesamiento de tranSACiones a nivel de usuario/cliente.	Errores operativos por parte del usuario (registro de información errada)
			Fallas en las conexiones de red o en equipo de computo
			Fallas eléctricas (a partir de 2 horas).
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debido errores en la integridad de los datos	Falta de soporte realizado al sistema Integrado de Información Financiera
			No llevar un control de la historia del código fuente
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico	Problemas de conexión o servidor del servicio que brinda el proveedor
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor	No generación de copias de respaldo (cuentas creadas, permisos y configuración)
			Capacidad de almacenamiento limitada
			Borrado de cuentas por accesos no autorizados por personal que administra el correo
			Bajo nivel de complejidad del contraseñas de correo vía acceso-pagina web
10	Equipos de cómputo terminales de ventanilla y analistas de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio	Personal no capacitado para el mantenimiento de equipos de computo
			No se ha determinado la vida útil de los equipo
			Incumplimiento del plan de mantenimiento de equipos.
			Fallas en sistema de alimentación eléctrica.
			Errores de configuración de los equipos
			Mal uso del equipo por parte del usuario
			Condiciones de ambientes inadecuadas
			No se tienen identificados los equipos críticos en caso de evacuación.
			El personal guarda información sensible en sus equipos y no las guarda en el servidor
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad
			Accesos no autorizado a la PC de Integración de Software
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema
			No complejidad de contraseñas en el respaldo de código fuente
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.	Registro - Inventario no adecuado de documentación
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.	Registro - Inventario no adecuado de documentación de requerimiento
14	Analistas de sistemas (Responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar.
		Pérdida de información sensible debido a fuga a través de correos electrónicos	Falta de monitoreo de envío y recepción de correos

		y/o páginas web	**Acceso total a la Web**
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software	**Plan de Inducción no adecuado**
15	**Equipos de cómputo del Área de Desarrollo (concentra toda la información de desarrollo y de configuración de las aplicaciones)**	**Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos**	**Acceso total a la Web**
16	**Backups o respaldos de desarrollo y mantenimiento**	**Reversión de adecuaciones a los sistemas, no es posible.**	**No se trasladan copias de respaldo en sitios alternos**

3.5. DETERMINACIÓN DEL APETITO Y LA TOLERANCIA AL RIEGO DE TI

Las Microfinancieras de Chiclayo ha planteado los siguientes objetivos estratégicos u operacionales, clasificados en las siguientes cuatro perspectivas:

A. Mejora de la gestión de la cartera de créditos
B. Gestión financiera para el crecimiento
C. Mejorar el posicionamiento
D. Gestión del talento humano

La infraestructura tecnológica informática está directamente relacionada con dar soporte a los siguientes objetivos:

Tabla N° 23. Identificación de los objetivos estratégicos u operacionales soportados por TI

Objetivo Estratégico u Operacional de las Microfinancieras de Chiclayo	Estrategia relacionada con TI
Optimizar los procesos de gestión de cartera de créditos	- Gestionar proyectos de TI para dar soporte a nuevos productos y servicios de créditos - Perfeccionar las aplicaciones informáticas para la supervisión y control con fines de minimizar los riesgos operacionales. - Implementar sistemas de comunicación robustos para las nuevas oficinas
Aplicar mecanismos y herramientas para monitorear y reducir costos operativos	- Gestionar proyectos de TI para implementación de controles de TI como mecanismo de seguimiento, trazabilidad y reacción oportuna frente a amenazas
Fidelizar clientes a través del servicio	- Asegurar la continuidad de los servicios de TI a través de la disponibilidad operativa de a infraestructura física de TI - Aseguramiento de la integridad y oportunidad de la información relacionadas a las cuentas de cliente - Implementar servicios de soporte basados en buenas prácticas como ITIL y COBIT: gestión de incidentes, gestión de problemas, gestión de configuraciones, gestión de cambios, gestión de niveles de Servicios
Fidelizar de personal con la seguridad de la información	- Capacitación del personal de TI y los usuarios de TI - Concientización del personal en material de seguridad de la información - Plan de incentivos y sanciones en materia de cumplimiento de políticas de seguridad de TI, gestión de riesgos y continuidad de procesos de TI

A continuación se determina el apetito y tolerancia al riesgo para cada uno de los objetivos estratégicos u operacionales relacionados con TI.

Tabla N° 24. Determinación del apetito y la tolerancia al riesgo de TI por cada objetivo estratégico u operacional

Objetivo Estratégico u Operacional de las Microfinancieras de Chiclayo	Optimizar los procesos de gestión de cartera de créditos	
Apetito de riesgo	– puede sea causa de incumplimiento leve o técnico de una ley o regulación – puede sea causa de una merma en la seguridad o dificulte la investigación de un incidente – efectos de bajo interés para la competencia. – efectos de bajo valor comercial – puede que cause la interrupción de actividades propias de las Microfinancieras de Chiclayo – dificulte la investigación o facilite la comisión de delitos – 1 hora < RTO < 4 horas	
Tolerancia de riesgo	– probablemente sea causa de incumplimiento de una ley o regulación – puede sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves – **de cierto interés para la competencia** – causa de pérdidas financieras o merma de ingresos – posiblemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo con impacto en otras organizaciones o en los clientes – Dificulte la investigación o facilite la comisión de delitos – 4 horas < RTO < 1 día	
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI	Mayor	Probable
Relacionados con el personal de TI	Moderado	Posible
Gestión de proyectos	Mínimo	Raro
Gestión de la seguridad	Mínimo	Posible
Entrega y soporte de servicios de TI	Catastrófico	Casi seguro
Aplicaciones	Catastrófico	Casi seguro
Otros escenarios	Mayor	Probable

Objetivo Estratégico u Operacional de las Microfinancieras de Chiclayo	Aplicar mecanismos y herramientas para monitorear y reducir costos operativos
Apetito de riesgo	– puede ser causa de incumplimiento leve o técnico de una ley o regulación – posiblemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente – probablemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo – probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
Tolerancia de riesgo	– probablemente sea causa de incumplimiento de una ley o regulación – probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves – probablemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo con impacto en otras organizaciones o en los clientes

	– probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local – probablemente impediría la operación efectiva de más de una parte de las Microfinancieras de Chiclayo	
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI	Catastrófico	Casi seguro
Relacionados con el personal de TI	Mínimo	Raro
Gestión de proyectos	Moderado	Posible
Gestión de la seguridad	Mayor	Probable
Entrega y soporte de servicios de TI	Mínimo	Posible
Otros escenarios	Mayor	Probable

Objetivo Estratégico u Operacional de las Microfinancieras de Chiclayo	Fidelizar clientes a través del servicio	
Apetito de riesgo	– de bajo interés para la competencia. de bajo valor comercial – probablemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo – probablemente impediría la operación efectiva de una parte de las Microfinancieras de Chiclayo – probablemente afecte negativamente a las relaciones internas de las Microfinancieras de Chiclayo – dificulte la investigación o facilite la comisión de delitos – 1 hora < RTO < 4 horas	
Tolerancia de riesgo	– **de cierto interés para la competencia** – causa de pérdidas financieras o merma de ingresos – probablemente cause la interrupción de actividades propias de las Microfinancieras de Chiclayo con impacto en otras organizaciones o en los clientes – probablemente impediría la operación efectiva de más de una parte de las Microfinancieras de Chiclayo – 4 horas < RTO < 1 día	
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI	Mayor	Posible
Relacionados con el personal de TI	Mayor	Probable
Gestión de proyectos	Mínimo	Raro
Gestión de la seguridad	Moderado	Posible
Entrega y soporte de servicios de TI	Catastrófico	Casi seguro
Otros escenarios	Moderado	Posible

Objetivo Estratégico u Operacional de las Microfinancieras de Chiclayo	Fidelizar de personal con la seguridad de la información
Apetito de riesgo	– probablemente sea causa de incumplimiento leve o técnico de una ley o regulación – probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente – probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local) – probablemente impediría la operación efectiva de una parte de las Microfinancieras de Chiclayo – dificulte la investigación o facilite la comisión de delitos
Tolerancia de riesgo	– probablemente sea causa de incumplimiento de una ley o regulación

	– probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves – probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local – probablemente impediría la operación efectiva de más de una parte de las Microfinancieras de Chiclayo	
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física de TI	Mínimo	Improbable
Relacionados con el personal de TI	Catastrófico	Probable
Gestión de proyectos	Insignificante	Improbable
Gestión de la seguridad	Mayor	Posible
Entrega y soporte de servicios de TI	Mínimo	Raro
Otros escenarios	Moderado	Probable

3.6. VALORACIÓN DEL IMPACTO Y PROBABILIDAD DE OCURRENCIA DE LAS AMENAZAS

Para la valoración del impacto y probabilidad de ocurrencia, y en consecuencia, para obtener el nivel de riesgo al que está expuesto cada activo de TI en Las Microfinancieras de Chiclayo, se realizó un levantamiento de información para evaluar los controles existentes actualmente y la efectividad de su implementación. Esta información se registra en el Anexo N° 02 y fue obtenida a través de entrevistas, observación directa y testeos de penetración (en la medida que fue permitido).

Los resultados de las valoraciones para los impactos y probabilidad de ocurrencia de cada amenaza para cada activo de TI; así como la obtención del nivel de riesgo intrínseco (usando los formatos y niveles de valoración de las tablas N° 11, 12, 14 y 15), se muestran en la siguiente tabla**:**

Tabla N° 25: Valoración del Nivel de Riesgo Intrínseco (NRI)

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
1	Servidor principal de dominio	Paralización de procesos y actividades del negocio, no se accede a los servicios de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio	3	Moderado	2	Improbable	R1	2	Bajo
			Falla en los componentes físicos	4	Mayor	3	Posible	R2	3	Medio
			Fallas en el sistema operativo, falta de actualización de parches	5	Catastrófico	4	Probable	R3	5	Muy alto
			No se cuenta con un plan de mantenimiento de los servidores	3	Moderado	2	Improbable	R4	2	Bajo
			Ataque de virus	2	Menor	2	Improbable	R5	2	Bajo
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible (datos de clientes)	Administrador tiene acceso total a la base de datos y puede realizar modificaciones	4	Mayor	4	Probable	R6	4	Alto
			Deficiencia en el diseño de base datos (normalización de BD).	2	Menor	3	Posible	R7	2	Bajo
			Usuarios acceden a servidor de base de datos por canales no autorizados	5	Catastrófico	4	Probable	R8	5	Muy alto
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones	5	Catastrófico	3	Posible	R9	4	Alto
			Falla de la red de comunicaciones con otras agencias	4	Mayor	4	Probable	R10	4	Alto
			Fallas eléctricas que generen la interrupción de los procesos y servicios	4	Mayor	3	Posible	R11	3	Medio
			No se cuenta con servidor de firewall a nivel de hardware	3	Moderado	2	Improbable	R12	2	Bajo
4	Sala de servidores o Centro de Procesamiento Central	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores	5	Catastrófico	2	Improbable	R13	3	Medio
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.	2	Menor	3	Posible	R41	2	Bajo
		Pérdida de Activos de TI en la sala de servidores (costo de hardware /	No se mantiene un control o registro de acceso a las áreas restringidas	2	Menor	2	Improbable	R15	2	Bajo

		paralización de Operaciones)	Falta de un registro de acceso a la sala de servidores	3	Moderado	2	Improbable	R16	2	Bajo
			No se tiene una política y procedimiento para el personal que realiza mantenimiento en la institución	2	Menor	3	Posible	R17	2	Bajo
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento). Y revisión de maletines.	4	Mayor	3	Posible	R18	3	Medio
5	Bases de Datos	Multas y sanciones, Perdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD	4	Mayor	3	Posible	R19	3	Medio
			Existencia de passwords no adecuados para usuarios locales y de red	3	Moderado	2	Improbable	R20	2	Bajo
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente	3	Moderado	2	Improbable	R21	2	Bajo
			Acceso a la BD desde otras aplicaciones	4	Mayor	3	Posible	R22	3	Medio
			Virus informáticos	3	Moderado	3	Posible	R23	3	Medio
			Realización de copias no autorizadas de la Base de Datos.	4	Mayor	3	Posible	R24	3	Medio
			Modificación no autorizada de BD	5	Catastrófico	4	Probable	R25	5	Muy alto
		Falta de espacio de almacenamiento	Incremento de transacciones	3	Moderado	3	Posible	R26	3	Medio
			No existe un procedimiento de mantenimiento de a BD.	3	Moderado	2	Improbable	R27	2	Bajo
			Incremento de espacio por virus.	3	Moderado	1	Raro	R28	1	Muy bajo
6	Backups de base de datos	Paralización de procesos, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Fallas en los dispositivos de almacenamiento (disco duro del servidor)	4	Mayor	3	Posible	R29	3	Medio
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo	2	Menor	2	Improbable	R30	2	Bajo
			Errores en el proceso de generación de backups	5	Catastrófico	4	Probable	R31	5	Muy alto
			No se lleva un registro de la generación de backups	3	Moderado	3	Posible	R32	3	Medio
7	Personal de área de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos	Inadecuada segregación de funciones	3	Moderado	2	Improbable	R33	2	Bajo
			No existe un plan de capacitación adecuado	2	Menor	3	Posible	R34	2	Bajo

			Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)	2	Menor	3	Posible	R35	2	Bajo
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos	4	Mayor	3	Posible	R36	3	Medio
			Falta de control y seguimiento de accesos	5	Catastrófico	3	Posible	R37	4	Alto
			Falta de acuerdos de confidencialidad	4	Mayor	3	Posible	R38	3	Medio
			Impulsos mezquinos que hace que el personal actúe de manera anormal en el desarrollo de sus labores	3	Moderado	3	Posible	R39	3	Medio
			Falta de procedimiento de mantenimiento de usuarios	3	Moderado	2	Improbable	R40	2	Bajo
8	Aplicaciones informáticas de créditos y captaciones	Paralización de procesos debido a Problemas en el procesamiento de transacciones a nivel de usuario/cliente.	Errores operativos por parte del usuario (registro de información errada)	3	Moderado	3	Posible	R41	3	Medio
			Fallas en las conexiones de red o en equipo de computo	3	Moderado	3	Posible	R42	3	Medio
			Fallas eléctricas (a partir de 2 horas)	4	Mayor	3	Posible	R43	3	Medio
		Información brindada al personal del negocio para el desarrollo de los procesos del negocio es inexacta debido errores en la integridad de los datos	Falta de soporte realizado al sistema Integrado de Información Financiera	3	Moderado	2	Improbable	R44	2	Bajo
			No llevar un control de la historia del código fuente	4	Mayor	3	Posible	R45	3	Medio
9	Correo electrónico institucional	Retraso de actividades debido a Caídas del servicio de correo electrónico	Problemas de conexión o servidor del servicio que brinda el proveedor	3	Moderado	3	Posible	R46	3	Medio
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico por parte del proveedor	No generación de copias de respaldo (cuentas creadas, permisos y configuración)	3	Moderado	3	Posible	R47	3	Medio
			Capacidad de almacenamiento limitada	2	Menor	2	Improbable	R48	2	Bajo
			Borrado de cuentas por accesos no autorizados por personal que administra el correo	3	Moderado	2	Improbable	R49	2	Bajo
			Bajo nivel de complejidad del contraseñas de correo vía acceso-pagina web	3	Moderado	3	Posible	R50	3	Medio
10	Equipos de cómputo terminales de ventanilla y analistas de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio	Personal no capacitado para el mantenimiento de equipos de computo	4	Mayor	2	Improbable	R51	2	Bajo
			No se ha determinado la vida útil de los equipo	2	Menor	2	Improbable	R52	2	Bajo
			Incumplimiento del plan de mantenimiento de equipos	2	Menor	3	Posible	R53	2	Bajo

			Fallas en sistema de alimentación eléctrica	3	Moderado	3	Posible	R54	3	Medio
			Errores de configuración de los equipos	2	Menor	3	Posible	R55	2	Bajo
			Mal uso del equipo por parte del usuario	3	Moderado	4	Probable	R56	3	Medio
			Condiciones de ambientes inadecuadas	2	Menor	3	Posible	R57	2	Bajo
			No se tienen identificados los equipos críticos en caso de evacuación	3	Moderado	2	Improbable	R58	2	Bajo
			El personal guarda información sensible en sus equipos y no las guarda en el servidor	4	Mayor	4	Probable	R59	4	Alto
11	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción	No se realizan copias de seguridad	4	Mayor	2	Improbable	R60	2	Bajo
			Accesos no autorizado a la PC de Integración de Software	4	Mayor	2	Improbable	R61	2	Bajo
		Perdida de información, multas y sanciones por Manipulación de códigos fuente para beneficio del trabajador	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo)	4	Mayor	3	Posible	R62	3	Medio
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema	4	Mayor	3	Posible	R63	3	Medio
			No complejidad de contraseñas en el respaldo de código fuente	3	Moderado	3	Posible	R64	3	Medio
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso	5	Catastrófico	4	Probable	R65	5	Muy alto
12	Archivos de Actas de conformidad	Observaciones de entes supervisores sobre procesos que están en Producción no sustentados.	Registro - Inventario no adecuado de documentación	3	Moderado	3	Posible	R66	3	Medio
13	Archivo de requerimientos informáticos (físico)	Pérdida de información no permite el cumplimiento de Desarrollo de Requerimientos.	Registro - Inventario no adecuado de documentación de requerimiento	3	Moderado	3	Posible	R67	3	Medio
14	Analistas de sistemas (Responsables de la implementación de requerimientos)	Tiempo de desarrollo de requerimientos que exceden cronograma de actividades.	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio	2	Menor	4	Probable	R68	2	Bajo
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar	3	Moderado	3	Posible	R69	3	Medio

		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web	Falta de monitoreo de envío y recepción de correos	3	Moderado	2	Improbable	R70	2	Bajo
			Acceso total a la Web	4	Mayor	3	Posible	R71	3	Medio
		Pérdida de recursos debido a Implementaciones no acordes a metodología y estándares de desarrollo de software	Plan de Inducción no adecuado	2	Menor	2	Improbable	R72	2	Bajo
15	Equipos de cómputo del Área de Desarrollo	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos	Acceso total a la Web	3	Moderado	3	Posible	R72	3	Medio
16	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible	No se trasladan copias de respaldo en sitios alternos	5	Catastrófico	3	Posible	R74	4	Alto

3.7. DEFINICIÓN DE MÉTRICAS PARA GESTIÓN DE RIESGOS DE TI

Para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo de las Microfinancieras de Chiclayo (es decir, el nivel de riesgo que las Microfinancieras de Chiclayo está preparada para aceptar), y que a su vez tenga un impacto negativo, se realizará a través de métricas basadas en indicadores de riesgos clave (KRI).

El objetivo de estos indicadores, es que sirvan como variables que funcionen como alertas tempranas que avisen de los cambios en los perfiles de riesgo de TI que pudiesen ocurrir en las Microfinancieras de Chiclayo.

De acuerdo a RMA[1] las categorías de riesgos para una entidad financiera son:

- Riesgos de conciliación de cuentas
- Riesgos de Cambios
- Riesgo de Cumplimiento
- Riesgos de Desembolso
- Riesgo de Fraude
- Riesgo de Seguridad de la Información

Para cada una de estas categorías RMA define una serie de KRIs. Específicamente, las KRI que se plantean como métricas del modelo propuesto de gestión de riesgos de TI son los propuestos por RMA para los Riesgos de Seguridad de la Información, que son las que están directamente relacionadas con el objetivo de esta investigación. Adicionalmente se plantean

Tabla N° 26: Indicadores de riesgo clave propuestos para el modelo de gestión de riesgos

Indicador	Fuente	Frecuencia de medición
Número de personas que manejan información sensible de clientes	**Retail Banking KRI Working Group**	**Trimestral**
Número de ataques reportados por Seguridad Informática	**Retail Banking KRI Working Group**	**Trimestral**
Porcentaje de terceros donde haya excepciones o preocupaciones por la seguridad de la información	**Retail Banking KRI Working Group**	**Trimestral**
Número de derechos de acceso a los aplicativos por el personal (sobre el umbral)	**Retail Banking KRI Working Group**	**Trimestral**
Número de fallos relacionados con el sistema de TI y otros equipos	**Propio**	**Mensual**
Número de llamadas para ayudar escritorio en sistema informático y otra equipo	**Propio**	**Mensual**
Promedio de tiempo de inactividad del sistema de TI y otros equipos	**Propio**	**Mensual**
Aumento de la carga de transacciones en los sistemas	**Propio**	**Mensual**

[1] **Risk Management Association**

3.8. PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE ACUERDO A LA ISO/IEC 27001

Antes de la implementación de los controles y salvaguardas para tratar los niveles de riesgo no aceptados, primero se definieron e implementaron las políticas de seguridad de la información, las cuales se tomaron del marco de referencia ISO/IEC 27001 necesarias para lograr la implantación, cumplimiento y efectividad de cada uno de los controles propuestos.

Estas políticas de seguridad a implantar se detallan en el cuadro siguiente:

Tabla N° 27: Políticas de seguridad necesarias para la implementación de los controles

Clausula	Categoría de Seguridad	Nombre del Control	Descripción de la política
Política de Seguridad	Política de Seguridad de Información	Documentar política de seguridad de información	La Gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades importantes a la organización
		Revisión de la Política de Seguridad de Información	La Política de seguridad de la información debe ser revisada a intervalos planeados o si ocurren cambios importantes que aseguren la continuidad y eficiencia
Organización de la seguridad de la información	Organización Interna	Compromiso de la gerencia con la seguridad de la información	La alta gerencia debe apoyar activamente la seguridad dentro de la organización a través de un alinea clara, compromiso detallado y reconocimiento de responsabilidades en cuanto a seguridad de la información.
		Coordinación de la seguridad de la información	Las actividades de la seguridad de información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles relevante.
		Asignación de responsabilidades de la seguridad de la información	Se debe definir de manera clara la responsabilidad de la seguridad de la información.
		Proceso de autorización para los medios de procesamiento de información	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información.
		Acuerdos de confidencialidad	Se debe identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación reflejando las necesidades de la organización para la protección de la información.
	Entidades externas	Tratamiento de la seguridad cuando se interactúa con clientes	Se debe tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
Gestión de activos	Responsabilidad por la gestión de activos	Inventario de activos	Todos los activos deben estar claramente identificados y se debe elabora y mantener un inventario de todos los activos importantes.
		Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados.
	Clasificación de la información	Lineamientos de clasificación	La información debe ser clasificada de acuerdo a su valor, requerimientos legales, confidencialidad y grado crítico para la organización
		Etiquetado y manejo de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para etiquetar y manejar la información de acuerdo con el esquema de clasificación hecho por la organización
Gestión de incidentes en la seguridad de la información	Reporte de eventos y debilidades de la seguridad de la información	Reporte de eventos en la seguridad de la información	Los eventos en seguridad de la información deben reportarse a través de los canales gerenciales lo más rápido posible
		Reporte de debilidades en la seguridad	Se debe solicitar que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de la información tomen nota y reporten cualquier debilidad observada y/o sospecha en cuanto a seguridad de la información se refiere.
	Gestión de incidentes y mejoras en la	Responsabilidad y procedimientos	Se debe establecer las responsabilidades y procedimientos gerenciales, para asegurar la respuesta rápida, efectiva y ordenada a los incidentes a seguridad de la información.

	seguridad de la información	Aprendizaje en los incidentes de la seguridad de la información	Debe existir mecanismos para cuantificar y monitorear los tipos , volúmenes y costos en los incidentes en la seguridad de la información
		Recolección de evidencia	Cuando la acción de seguimiento contra una persona u organización después de un incidente, involucra una acción legal, se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en las jurisdicciones relevantes.
Cumplimiento	Cumplimiento con requerimientos legales	Protección de los registros organizacionales	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
		protección de la data y privacidad de información personal	Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
Gestión de las comunicaciones y operaciones	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
Control de acceso	Gestión del acceso al usuario	Revisión de los derechos de acceso del usuario	La alta gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Seguridad en los procesos de desarrollo y soporte	Desarrollo de outsourcing software	El desarrollo de software que ha sido outsourcing debe ser supervisado y monitoreado por la organización

3.9. IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD Y DE LAS ESTRATEGIAS DE SU IMPLANTACIÓN.

Luego de definir las políticas de seguridad que Las Microfinancieras de Chiclayo debería adoptar, se procedió a definir los controles para el tratamiento de los diversos riesgos identificados; especificando el control, su descripción según la norma ISO 27002, los riesgos que mitigará y la adaptación de dicho control con la realidad organizacional de Las Microfinancieras de Chiclayo.

Los resultados de esta actividad se muestran en el cuadro siguiente:

Tabla N° 28: Implementación de controles según el NRI calculado

Nivel de Riesgo Intrínseco (NRI)			Control		Estrategia de implementación
ID riesgo	Nivel	Categoría	ID Control	Descripción	
R1	2	Bajo	C1	Servicio de Mantenimiento por parte del fabricante correctivo	Evitar aumento del riesgo
R2	3	Medio	C2	Se cuenta con un servicio de mantenimiento por parte del fabricante	Evitar aumento del riesgo
			C3	Sala de servidores con controles ambientales	Evitar aumento del riesgo
R3	5	Muy alto	C4	Personal capacitado en administración de Windows server y actualizaciones de parches	Transferencia del riesgo a terceros
R4	2	Bajo	C5	Incluir en el Plan de mantenimiento a los servidores	Evitar aumento del riesgo
R5	2	Bajo	C6	Se cuenta con software antivirus instalado en toda la red y con actualizaciones automáticas	Evitar aumento del riesgo
			C7	Se cuenta con copias de seguridad de la BD	Evitar aumento del riesgo
			C8	Se cuenta con un servidor de backup	Evitar aumento del riesgo
			C9	Se tiene implementado un centro de cómputo alterno (CCA), el cual permite generar copias de respaldo en línea	Evitar aumento del riesgo
R6	4	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera bimensual las pistas de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD	Elección de controles
R7	2	Bajo	C11	En el proceso de desarrollo se cuenta con una fase de pruebas y revisión, donde se analizan el diseño de las tablas y de las modificaciones	Evitar aumento del riesgo
			C12	La Jefe de Producción, realiza un análisis de los ejecutables y códigos fuentes que pasa la División de desarrollo	Evitar aumento del riesgo
R8	5	Muy alto	C13	Se tiene establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos	Elección de controles

			C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales	Elección de controles
			C15	Los perfiles de usuarios que acceden a la base de datos tiene accesos restringidos	Elección de controles
R9	4	Alto	C16	Se cuenta con línea de contingencia para comunicaciones	Transferencia del riesgo a terceros
			C17	Reporte de averías al proveedor	Transferencia del riesgo a terceros
R10	4	Alto	C18	Reporte de averías al proveedor	Transferencia del riesgo a terceros
R11	4	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica	Elección de controles
			C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento	Elección de controles
			C21	Se cuenta con un plan de mantenimiento al sistema eléctrico	Elección de controles
R12	2	Bajo	C22	Se cuenta con firewall a nivel de software	Evitar aumento del riesgo
R13	3	Medio	C23	Se cuentan con políticas de seguridad	Evitar aumento del riesgo
			C24	Se registran los accesos a sala de servidores y el área de TI, mediante una bitácora de acceso	Evitar aumento del riesgo
			C25	Los accesos por parte de personal a realizar mantenimiento, se realiza acompañado de personal del área	Evitar aumento del riesgo
			C26	El acceso al ambiente de la sala de servidores, tiene acceso restringido mediante una puerta con llave. La llave la maneja únicamente el Jefe de Producción y Soporte y el Operador de Sistemas	Evitar aumento del riesgo
			C27	Sala de servidores se encuentra en un ambiente aislado al ambiente de producción y de Desarrollo	Evitar aumento del riesgo
			C28	Se tiene implementado una cámara de vigilancia que monitorea el ingreso de personas internas como externas al área de TI	Evitar aumento del riesgo
R14	2	Bajo	C29	Se cuenta con un equipo de aire acondicionado el cual no permite el recalentamiento de los equipos	Evitar aumento del riesgo
			C30	Se tiene instalado extintores y sensores de humo	Evitar aumento del riesgo
			C31	La sala de servidores se encuentra en un ambiente aislado al ambiente de Producción y de Desarrollo. Este ambiente cuenta con una puerta de acceso bajo llave	Evitar aumento del riesgo
			C32	Se cuenta con luces de emergencia	Evitar aumento del riesgo
			C33	Se registran los accesos a sala de servidores, mediante una bitácora	Evitar aumento del riesgo
			C34	Se cuenta con una cámara de vigilancia en la entrada al área de TI	Evitar aumento del riesgo
			C35	Se tiene designado personal para el manejo de llaves	Evitar aumento del riesgo
			C36	Se cuenta con sala de servidor alterno	Evitar aumento del riesgo
			C37	Mantenimiento de los equipos de seguridad	Evitar aumento del riesgo

			C38	Se cuenta con un plan de pruebas de los sensores por parte del personal de ASBANC	Evitar aumento del riesgo
R15	2	Bajo	C39	Se cuenta con vigilancia al ingreso a la institución, quién mediante su cuaderno de cargos registra al personal que ingresa a las zonas de acceso restringido (TI)	Evitar aumento del riesgo
R16	2	Bajo	C40	Se cuenta con una bitácora, donde el personal interno y externo que desea ingresar a la sala de servidores deberá registrar la hora de ingreso, salida y nombre	Evitar aumento del riesgo
R17	2	Bajo	C41	No se tienen controles	Evitar aumento del riesgo
R18	3	Medio	C42	Se cuenta con formatos de entrada salidas de para los equipos que el personal de las Microfinancieras de Chiclayo saca fuera de las instalaciones	Evitar aumento del riesgo
R19	4	Alto	C43	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios	Elección de controles
R20	2	Bajo	C44	Se permite la creación de contraseñas con un nivel de seguridad y complejidad, teniendo en cuenta caracteres numéricos y alfanuméricos.	Evitar aumento del riesgo
R21	2	Bajo	C45	Incluir en el Plan de trabajo de la oficialía de seguridad	Evitar aumento del riesgo
R22	4	Alto	C46	Se han deshabilitado acceso al Excel en todas las máquinas	Elección de controles
			C47	Acceso a la BD protegida por un password que es de conocimiento del jefe de área de producción y soporte	Elección de controles
R23	3	Medio	C48	Se realiza la actualización del antivirus en línea	Evitar aumento del riesgo
R24	3	Medio	C49	BD protegidas con clave y esta clave únicamente la conoce solo personal autorizado	Evitar aumento del riesgo
			C50	No se tiene carpetas compartidas de la BD	Elección de controles
R25	5	Muy alto	C51	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción	Elección de controles
R26	3	Medio	C52	La Jefe de Producción y Soporte supervisa de manera manual la disponibilidad de la capacidad del disco del servidor, a fin de que exista espacio suficiente para la BD	Evitar aumento del riesgo
R27	2	Bajo	C53	Se realiza un mantenimiento de la BD, pero no está documentado	Evitar aumento del riesgo
R28	1	Muy bajo	C54	Se cuenta con un antivirus que se actualiza en línea	Elección de controles
			C55	Puertos de control de acceso al servidor se encuentran bloqueados	Elección de controles
R29	4	Alto	C56	Se cuenta con políticas y procedimientos de generación de backups	Elección de controles
			C57	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno (Ag. Moshoqueque) y la otra en bóveda(Oficina Principal)	Elección de controles
			C58	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo	Elección de controles
			C59	Se realiza un monitoreo del procedimiento de respaldo de los backups	Elección de controles

			C60	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario	Elección de controles
R30	2	Bajo	C61	Se realiza una verificación de estado de almacenamiento y resguardo de los medios de respaldo.	Evitar aumento del riesgo
R31	5	Muy alto	C62	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos	Elección de controles
			C63	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación	Elección de controles
			C64	Se realiza la verificación periódica de las copias generadas	Elección de controles
R32	3	Medio	C65	Se cuenta con un cuaderno de cargos en el cual se consigna el envío de las copias de respaldo por fechas de generación, responsable de envío y recepción, tanto en el CCP como en la agencia Moshoqueque.	Evitar aumento del riesgo
R33	2	Bajo	C66	Se cuenta con manual de organización y funciones en el que se tiene establecido las responsabilidades que debe cumplir el personal en la operativa diaria	Evitar aumento del riesgo
R34	2	Bajo	C67	Existe un plan de capacitación presentado por el jefe de TI	Evitar aumento del riesgo
R35	2	Bajo	C68	Se tiene personal de reemplazo, pero no está totalmente capacitado en las actividades diarias.	Evitar aumento del riesgo
R36	4	Alto	C69	La asignación de privilegios va de acuerdo al manual de funciones	Elección de controles
			C70	Se generan pistas de auditoria que son revisadas periódicamente	Elección de controles
R37	4	Alto	C71	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos	Elección de controles
R38	4	Alto	C72	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados	Elección de controles
R39	3	Medio	C73	Al inicio de la relación laboral, se realizan evaluaciones psicológicos al personal y evaluación de historial	Evitar aumento del riesgo
			C74	Se cuenta con políticas de seguridad y se cuenta con reglamentos internos que establecen sanciones	Evitar aumento del riesgo
R40	2	Bajo	C75	Se cuenta con reglamento de altas, bajas y modificación de usuarios.	Evitar aumento del riesgo
R41	3	Medio	C76	Existen validaciones en el sistema para el registro de información. Esta validación se ha determinado a nivel de base de datos	Evitar aumento del riesgo
			C77	En los perfiles del puesto, se ha designado como requisito que el personal cuente con conocimientos básicos de computación	Evitar aumento del riesgo
R42	3	Medio	C78	Se cuenta con equipos de respaldo de cómputo y soporte técnico (interno), además de asignar una categoría de urgencia de equipos	Evitar aumento del riesgo
			C79	Se cuenta con personal técnico externo	Evitar aumento del riesgo
			C80	Personal interno puede resolver problemas hasta cierto nivel de complejidad	Evitar aumento del riesgo
R43	3	Medio	C81	Se cuenta con grupo electrógeno y un sistema de alimentación ininterrumpida (UPS)	Evitar aumento del riesgo
R44	2	Bajo	C82	Se da soporte de mantenimiento basado en requerimientos de los usuarios y mejoras de los procesos existentes de manera continua	Evitar aumento del riesgo

R45	3	Medio	C83	Toda versión del sistema de información histórica se encuentra documentado en files	Evitar aumento del riesgo
R46	3	Medio	C84	Se comunica vía telefonía la incidencia presentada	Evitar aumento del riesgo
R47	3	Medio	C85	El proveedor genera copias de respaldo de las configuraciones de los correos	Evitar aumento del riesgo
R48	2	Bajo	C86	Se revisa el estado de almacenamiento en el hosting de correo y se asigna cuota por cuenta de acuerdo al tipo de usuario	Evitar aumento del riesgo
R49	2	Bajo	C87	Se actualiza las contraseñas, cuando el personal que administró el correo ya no forma parte de la institución	Evitar aumento del riesgo
			C88	Se firma un acuerdo de confidencialidad	Evitar aumento del riesgo
R50	3	Medio	C89	Se tiene un reglamento de uso de correo, donde se establecen indicaciones para la creación de contraseñas	Evitar aumento del riesgo
R51	2	Bajo	C90	Se cuenta con un proceso de evaluación del personal nuevo por parte de Recursos Humanos	Evitar aumento del riesgo
			C91	Se cuenta con una lista de técnicos que permiten realizar el mantenimiento de los equipos	Evitar aumento del riesgo
			C92	La empresa proveedora, brinda servicios de mantenimiento a los equipos arrendados	Evitar aumento del riesgo
R52	2	Bajo	C93	Los equipos de cómputo se han arrendado a un proveedor por un periodo de tres años; asimismo se ha firmado un acuerdo un acuerdo de niveles de servicio con el arrendador	Evitar aumento del riesgo
R53	2	Bajo	C94	Se realiza un seguimiento al cumplimiento del plan por parte de la persona responsable de Continuidad del Negocio y el seguimiento es reportado en el informe de Continuidad de Negocio de manera bimensual	Evitar aumento del riesgo
R54	3	Medio	C95	Existe un plan de mantenimiento del sistema eléctrico, este mantenimiento se realiza de manera semestral	Evitar aumento del riesgo
			C96	Se cuenta con una red eléctrica estabilizada	Evitar aumento del riesgo
			C97	las PCs de misión crítica están conectadas a UPS	Evitar aumento del riesgo
			C98	Se realizan pruebas periódicas del sistema de respaldo eléctrico (UPS, Grupo electrógeno y motor)	Evitar aumento del riesgo
			C99	Se realiza mantenimiento programado a los equipos eléctricos	Evitar aumento del riesgo
R55	2	Bajo	C100	Se cuenta con personal capacitado para realizar las configuraciones de los equipos.	Evitar aumento del riesgo
R56	3	Medio	C101	En el MOF indica: Es responsabilidad de los usuarios, que el buen uso y conservación de los bienes o activos que las Microfinancieras de Chiclayo asigna al trabajador	Evitar aumento del riesgo
R57	2	Bajo	C102	Existe un ambiente para la ubicación de los equipos, así mismo estos ambientes cuentan con ambientes de ventilación.	Evitar aumento del riesgo
R58	2	Bajo	C103	Se tienen identificados los equipos críticos del área de TI y centro de cómputo Principal	Evitar aumento del riesgo
			C104	Se cuenta con políticas para la clasificación de la información	Evitar aumento del riesgo
R59	4	Alto	C105	Política de escritorios y pantallas limpias	Elección de controles
R60	2	Bajo	C106	Se realizan copias de seguridad de manera semanal, así mismo se lleva un control de los backups	Evitar aumento del riesgo
			C107	Se mantiene tres copias de respaldo (Of. Principal. Moshoqueque y Sección de desarrollo)	Evitar aumento del riesgo
R61	2	Bajo	C108	Seguridad de acceso local de usuario	Evitar aumento del riesgo
			C109	La pc de integración de desarrollo está separada de la red de producción	Evitar aumento del riesgo

			C110	Se generar copias de seguridad del código fuentes// existe registro de versiones	Evitar aumento del riesgo
R62	4	Alto	C111	El código fuente es clasificada como información restringida y controlada por el Jefe de TI	Elección de controles
R63	4	Alto	C112	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato	Elección de controles
			C113	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas	Elección de controles
			C114	Control de calidad por parte de la División de producción antes de su implantación	Elección de controles
R64	3	Medio	C115	Se ha asignado un complejidad en la contraseñas teniendo en caracteres y números, la contraseña cambia en cada respaldo	Evitar aumento del riesgo
R65	5	Muy alto	C116	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	Elección de controles
			C117	El especialista en sistemas de Información puede detectar cambios no programados	Elección de controles
			C118	Existe una fase de prueba en desarrollo y certificación antes del pase a producción	Elección de controles
R66	3	Medio	C119	Se cuenta con file de versiones en donde se adjuntan los requerimientos de los usuarios, control de cambios, manuales de usuarios, conformidades y otra documentación según corresponda el tipo de requerimiento	Evitar aumento del riesgo
R67	3	Medio	C120	Se mantiene un listado de inventario denominado matriz de requerimientos	Evitar aumento del riesgo
R68	2	Bajo	C121	Al ingresar cada analista de sistemas recibe inducción sobre los procesos del negocio y de los procesos automatizados de negocio. Asignación de tareas de manera gradual. Asignación de requerimientos teniendo en cuenta el nivel de experiencia en el desarrollo del proceso del negocio.	Evitar aumento del riesgo
R69	3	Medio	C122	Se priorizan los requerimientos de implementación de procesos más importantes	Evitar aumento del riesgo
R70	2	Bajo	C123	Existe reglamento específico de acceso a Internet	Evitar aumento del riesgo
R71	4	Alto	C124	Existe restricción de acceso a Internet según niveles de acceso de usuarios	Elección de controles
R72	2	Bajo	C125	Se realiza un proceso de inducción de los proceso del negocio y de los procesos automatizados en el sistema.	Evitar aumento del riesgo
R73	3	Medio	C126	Instalación de Antivirus	Evitar aumento del riesgo
R74	4	Alto	C127	Se mantiene un inventario de los backups generados, asi mismo se generan tres copias de respaldo que son enviados al sitio alterno	Elección de controles

3.10. Valorización del riesgo residual y determinación de la brecha de seguridad

Definidos los controles que se han implementado, corresponde la evaluación de su efectividad, para determinar el Nivel de Riesgo Residual (NRR) y por consiguiente determinar la brecha de seguridad para lograr los niveles de riesgo aceptables por Las Microfinancieras de Chiclayo. De acuerdo al apetito de riesgo definido, sólo se evaluarán los niveles de riesgo que hayan obtenido valores de "Alto" y "Muy alto".

Esta evaluación se realizó luego de diseñados e implementados formalmente los controles. Los resultados de la segunda evaluación se muestran en el cuadro siguiente:

Tabla N° 29: Valorización del NRR y determinación de la brecha de seguridad

Nivel de Riesgo Intrínseco (NRI)		Control Implantado		Valorización del Nivel de riesgo Residual (NRR)						Apetito de riesgo
ID riesgo	Categoría	ID Control	Descripción	Nivel	Categoría	Nivel	Categoría	Nivel	Categoría	
R3	Muy alto	C4	Personal capacitado en administración de Windows server y actualizaciones de parches	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R6	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera bimensual las pistas de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R8	Muy alto	C13	Se tiene establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos	5	Catastrófico	2	Improbable	3	Medio	Riesgo aceptable
		C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales							Riesgo aceptable
		C15	Los perfiles de usuarios que acceden a la base de datos tiene accesos restringidos							Riesgo aceptable
R9	Alto	C16	Se cuenta con línea de contingencia para comunicaciones	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
		C17	Reporte de averías al proveedor							Riesgo aceptable
R10	Alto	C18	Reporte de averías al proveedor	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R11	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica	4	Mayor	4	Probable	4	Alto	Riesgo NO aceptable
		C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento							Riesgo aceptable
		C21	Se cuenta con un plan de mantenimiento al sistema eléctrico							Riesgo aceptable
R19	Alto	C43	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
R22	Alto	C46	Se han deshabilitado acceso al Excel en todas las máquinas	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
		C47	Acceso a la BD protegida por un password que es de conocimiento del jefe de área de producción y soporte							Riesgo aceptable
		C50	No se tiene carpetas compartidas de la BD							Riesgo aceptable
R25	Muy alto	C51	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R29	Alto	C56	Se cuenta con políticas y procedimientos de generación de backups	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
		C57	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno (Ag. Moshoqueque) y la otra en bóveda(Oficina Principal)							Riesgo aceptable
		C58	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo							Riesgo aceptable
		C59	Se realiza un monitoreo del procedimiento de respaldo de los backups							Riesgo aceptable

		C60	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario							Riesgo aceptable
R31	Muy alto	C62	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
		C63	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación							Riesgo aceptable
		C64	Se realiza la verificación periódica de las copias generadas							Riesgo aceptable
R36	Alto	C69	La asignación de privilegios va de acuerdo al manual de funciones	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
		C70	Se generan pistas de auditoria que son revisadas periódicamente							Riesgo aceptable
R37	Alto	C71	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
R38	Alto	C72	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
R59	Alto	C105	Política de escritorios y pantallas limpias	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
R62	Alto	C111	El código fuente es clasificada como información restringida y controlada por el Jefe de TI	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R63	Alto	C112	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
		C113	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas							Riesgo aceptable
		C114	Control de calidad por parte de la División de producción antes de su implantación							Riesgo aceptable
R65	Muy alto	C116	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	4	Mayor	4	Probable	4	Alto	Riesgo NO aceptable
		C117	El especialista en sistemas de Información puede detectar cambios no programados							Riesgo aceptable
		C118	Existe una fase de prueba en desarrollo y certificación antes del pase a producción							Riesgo aceptable
R71	Alto	C124	Existe restricción de acceso a Internet según niveles de acceso de usuarios	3	Moderado	2	Improbable	2	Bajo	Riesgo aceptable
R74	Alto	C127	Se mantiene un inventario de los backups generados, así mismo se generan tres copias de respaldo que son enviados al sitio alterno	3	Moderado	2	Improbable	2	Bajo	Riesgo aceptable

IV. DISCUSIÓN DE RESULTADOS

4.1. CARACTERIZACIÓN DE LA DISCUSIÓN DE RESULTADOS

De acuerdo a la descripción dada en el diseño de la investigación observamos la necesidad de definir, desarrollar y proponer una metodología y una forma estructurada que permita evaluar objetivamente el diseño y la efectividad del modelo propuesto cuando se realizan las actividades de gestión de riesgos y evaluación de la continuidad de los procesos en la entidad tomada como caso de estudio.

Para atender y solucionar esta necesidad, se aplicó la siguiente metodología que permite relacionar variables cuantitativas y cualitativas a partir de los pesos asignados por las personas que tienen autoridad y desempeñan funciones de gestión de riesgos y de la continuidad de procesos en Las Microfinancieras de Chiclayo durante la evaluación, con el fin de valorar objetivamente la efectividad en el diseño y la efectividad del modelo propuesto. La metodología propuesta para evaluar el diseño y la efectividad del modelo propuesto es aplicable a todas las Cajas Rurales y su implementación depende del tamaño del negocio. Para efectos del ejercicio práctico que presentamos más adelante.

Para la aplicación de la metodología de evaluación del modelo propuesto se utilizó el Método Delphi.

Con el método “Delphi” obtuvimos la opinión y el conocimiento de las personas encargadas de las funciones de:

- Jefatura de TI
- Jefatura de la Unidad de Riesgos
- Oficialía de Seguridad de TI y de la Información
- Jefatura de la Unidad de Continuidad de negocio
- Auditor interno

Para su aplicación se consideró las siguientes características:

- Anonimato: Durante su aplicación ninguna de las personas que evaluaron el modelo supieron que los otros también estaban evaluando el modelo. Esto permitió que ninguna de los evaluadores del modelo sea influenciado por el conocimiento y experiencia de otro.
- Iteración y realimentación controlada: La iteración se consiguió al presentar el mismo cuestionario a todos los evaluadores de forma independiente.
- Respuesta del grupo: La información que se presenta a los evaluadores no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo obtenido.

El procedimiento realizado fue el siguiente:

1. Se elaboró un cuestionario tomando como base las variables consideradas en el cuadro de “Variables de contrastación de hipótesis”

2. Conseguir su compromiso de colaboración. Las personas elegidas conocen del tema y del modelo propuesto. Sin embargo, se socializó y explicó de forma individual al panel de personas seleccionadas, la metodología y los modelos propuestos.

3. Se determinó el contexto y el horizonte temporal (tiempo de aplicación) para la aplicación del cuestionario. En este caso la metodología y modelos propuestos fueron utilizados durante tres.

4. Posteriormente, se les envío a través de correo electrónico, un archivo con los cuestionarios diseñados en hojas electrónicas, que contienen los niveles, factores y variables definidas a través de preguntas, para que cada uno de ellos comparta sus opiniones sobre la relevancia del modelo propuesto en este trabajo. La asignación de la relevancia por parte del "experto", se realiza respondiendo "sí" o "no" a cada factor y variable del cuestionario y la asignación de los pesos, la realiza mediante el análisis y aplicación del criterio profesional y su función dentro de Las Microfinancieras de Chiclayo, asignando o distribuyendo un peso porcentual utilizando la escala de (0% al 100%) para cada pregunta, rango, evento y nivel que conforman las variables.

4.2. DISEÑO DEL CUESTIONARIO ENVIADO AL PANEL DE PERSONAS SELECCIONADAS PARA ASIGNAR PESOS A LOS FACTORES, VARIABLES Y NIVELES DEL MODELO PROPUESTO

a. Cuestionario para la Prueba de la Efectividad del Diseño:
   Objetivo: Probar la efectividad del diseño del modelo propuesto determinando si los controles de la entidad son operados como fue prescrito por las personas que poseen la autoridad y competencias necesarias para desempeñar la gestión de la seguridad, el control y la gestión de riesgos y, si satisfacen los objetivos de control exigidos por la SBS para prevenir o detectar riesgos de TI. (Ver Anexo N° 01)
b. Cuestionario para la Prueba de la Efectividad del Operación:
   Objetivo: Probar la efectividad de la operación del modelo propuesto determinando si está operando tal y como fue diseñado y si las personas que desempeñan la gestión de la seguridad, el control y la gestión de riesgos posee las competencias necesarias para desempeñar el control de manera efectiva. (Ver Anexo N° 01)

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 N° 30: Pesos para la calificación de los indicadores en los cuestionarios

Peso	Significado	Color
1	CLAVE	
2	RELEVANTE	
3	ESTÁNDAR	
4	IRRELEVANTE	

Leyenda

Clave: El indicador evaluado del modelo propuesto es importante considerarlo en el Sistema de Gestión de Seguridad de la Información de Las Microfinancieras de Chiclayo, porque cumple con los requisitos exigidos en la normativa la SBS.

Relevante: El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de Las Microfinancieras de Chiclayo, porque cumple con los requisitos exigidos en la normativa la SBS.

Estándar: El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de Las Microfinancieras de Chiclayo, con algunas modificaciones y mejoras para cumplir con los requisitos exigidos en la normativa la SBS.

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 Seguridad de la Información de Las Microfinancieras de Chiclayo.

4.3. RESULTADOS OBTENIDOS:

Los resultados del análisis Delphi se muestran en las siguientes tablas:

Tabla N° 31: Resultado de la evaluación de los factores y variables para probar la efectividad del diseño del modelo propuesto

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Información		Jefe Continuidad procesos		Auditor Interno		TOTALES	
Variable		Factor Relevante (indicador)	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso
Perspectiva: Gestión de riesgos de TI														
Estructuración de la metodología de análisis y tratamiento de riesgos	1	**Se ha definido nítidamente las categorías – como disponibilidad, integridad y confidencialidad – en las que se pueden agrupar los riesgos de TI**	**SI**	2	**SI**	2	**SI**	1	**SI**	2	**SI**	2	**100%**	2
	2	**La gestión de riesgos de TI se integra en la gestión de riesgos general para todos los riesgos a nivel corporativo**	**SI**	2	**SI**	2	**SI**	1	**SI**	2	**NO**	4	**80%**	2
	3	**Su estructura está diseñada para que los empleados relacionados con la gestión de la seguridad de TI y de riesgos puedan entenderlo y alcanzar el grado de cultura y concientización deseado**	**SI**	2	**SI**	3	**SI**	2	**SI**	3	**SI**	2	**100%**	2
Gobierno de los riesgos de TI	4	**Contempla todas las variables necesarias exigidas por la SBS para su evaluación**	**SI**	2	**SI**	2	**SI**	2	**SI**	2	**SI**	3	**100%**	2
	5	**Se ha establecido pautas para evaluar la magnitud de los riesgos de modo coherente**	**SI**	2	**SI**	3	**SI**	3	**SI**	2	**NO**	4	**80%**	3
	6	**Se cuenta con indicadores clave para monitorizar periódicamente la eficacia de nuestras actividades de gestión de riesgos de TI**	**SI**	3	**SI**	3	**SI**	2	**SI**	2	**SI**	2	**100%**	2
TOTAL (%)			**100%**		**100%**		**100%**		**100%**		**67%**		**93%**	

Tabla N° 32: Resultado de la evaluación de los Factores y variables para probar la efectividad de la operación del modelo propuesto

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Info		Jefe Continuidad procesos		Auditor Interno		TOTALES	
Variable		Factor Relevante (indicador)	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso
Perspectiva: Gestión de riesgos de TI														
Análisis y tratamiento de riesgos	1	**A partir del modelo propuestos se puede establecer un proceso formal y coherente para evaluar periódicamente potenciales riesgos de TI**	**SI**	2	**SI**	2	**SI**	2	**SI**	2	**SI**	2	**100%**	2
	2	**Se puede determinar con efectividad los niveles de riesgos inherentes de TI**	**NO**	2	**SI**	2	**SI**	2	**SI**	2	**SI**	2	**80%**	2
	3	**Se puede evaluar la efectividad de los controles y hacer seguimiento de las brechas de seguridad**	**SI**	2	**NO**	4	**SI**	2	**SI**	2	**NO**	4	**60%**	3
Gobierno de los riesgos de TI	4	**La información resultante del modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la gestión de riesgos de TI**	**SI**	2	**SI**	2	**SI**	3	**SI**	2	**SI**	3	**100%**	2
	5	**La información resultante del modelo sirve para tomar decisiones con efectividad en relación a las inversiones e importancia de los controles de seguridad**	**NO**	4	**NO**	4	**NO**	4	**NO**	4	**NO**	4	**0%**	4
TOTAL (%)			**60%**		**60%**		**80%**		**80%**		**60%**		**68%**	

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Con la correcta identificación de los procesos críticos de las microfinancieras, que ha partido principalmente de los dueños de los procesos, con su correspondiente priorización, se ha logrado identificar la infraestructura de TI más crítica y aplicar las estrategias para su recuperación y continuidad, lo que ha conllevado a disminuir el número de caídas o problemas.

Se ha logrado implementar un modelo de gestión de riesgos de TI, que identifica, evalúa y trata nítidamente los activos de TI, sus amenazas, debilidades y niveles de riesgo relacionadas con las categorías: disponibilidad, integridad y confidencialidad de la información, que exige la SBS para este tipo de organizaciones en sus planes de seguridad. Esto ha permitido lograr establecer pautas para evaluar la magnitud de los riesgos de modo coherente y contar con indicadores clave para monitorizar periódicamente la eficacia de las actividades de gestión de riesgos de TI en Las Microfinancieras de Chiclayo, mediante la evaluación de brechas de efectividad de los controles de seguridad de la información.

El producto tangible de la metodología de gestión de riesgos es la matriz de riesgos y a través de ella se ha logrado disponer de un registro permanentemente y actualizado de los principales activos de TI a proteger, de modo que se garantice la continuidad operativa vía los planes mitigación, de los riesgos inmersos en cada activo.

Queda demostrado que la metodología de gestión de riesgos y de continuidad de los procesos de TI, permite identificar los niveles de riesgos de tal forma que sirve de información para la toma de decisiones en relación la inversión para la implementación de los controles que sirvan de salvaguardas en la protección del proceso contra posibles amenazas y vulnerabilidades.

5.2. RECOMENDACIONES

Dado que la evaluación de los riesgos es permanente se recomienda que el modelo de matriz de riesgos que se propone sea implementado en una aplicación informática, que permita actualizaciones más dinámicas, con posibilidades de generar indicadores/resultados gráficos y generación de escenarios.

Es conveniente que la oficialía de la seguridad de la información designe responsabilidades que permitan, mediante una aplicación de la propuesta metodológica, alimentar permanentemente de la información necesaria por los verdaderos dueños de los procesos: lista de procesos/servicios críticos, activos, riesgos, amenazas, vulnerabilidades, controles, etc., de tal forma que permita obtener rápidamente la información del nivel de criticidad de sus procesos,

VI. REFERENCIAS BIBLIOGRÁFICAS

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

Alvarez Sosa, Yenny Maribel. (2013).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).

Avalos Ruiz, C. (2012). Análisis, diseño e implementación del sistema de riesgo operacional para entidades financieras. *Tesis*. Lima, Perú: Pontificia Universidad Católica del Perú - PUCP.

Campos, J., & Herrera, F. (2007). Políticas de seguridad organizacional y control de activos según la Norma Técnica Peruana NTP-ISO/IEC 17799 en la Oficina Central de Informática de la Universidad Nacional Pedro Ruiz Gallo. *Tesis*. Lambayeque, Peru: Universidad Nacional Pedro Ruiz Gallo.

Córdova Rodriguez, N. E. (2009). Plan de seguridad para una entidad financiera. *Tesis*. Lima, Perú: Universidad Nacional Mayor de San Marcos.

Costas Santos, J. (2011). *Seguridad informática.* Bogotá: Editorial Ra-ma.

Gartner INC. (Abril de 2013). *Is Your IT Security Budget Immature?* Obtenido de Gartner WebSite: http://www.gartner.com/technology/metrics/

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

IBM. (Abril de 2013). *La gestión de riesgos de TI*. Obtenido de IBM Compañy WebSite: http://www.935.ibm.com/services/es/cio/pdf/gestion-riesgos-ti-unos-sistemas-informacion-maduros-pueden-generar-grandes-resultados.pdf

ISACA. (2012). *COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* ISACA - Information Systems Audit and Control Association. ISACA.

ISACA, Asociación de Auditoria y Control de Sistemas de Información. (2005). *Manual de preparación al examen CISA* (15ava ed.). Madrid.

ISACA, Asociación de Auditoria y Control de Sistemas de Información. (2009). Lineamientos para la gestión de la seguridad de TI. *Manual de preparación CISA 2009*. Lima, Perú.

Medina, A. (2007). *Seguridad informática.* Lima: Universidad Nacional Mayor de San Marcos.

Peña, G., & Peña, L. (2005). Gestión de riesgo tecnológico. En *Mejores prácticas y estándares internacionales en gestión de riesgos y control interno.*

Superintendencia de Banca, Seguros y AFP.(2009) Reglamento para la Gestión del Riesgo Operacional. Lima Peru.

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

Vásquez, Karina del Rocío Gaona. (2013) 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.

ANEXOS

ANEXO N° 01

TABLAS DE FACTORES Y VARIABLES DE EVALUACIÓN DEL MODELO PROPUESTO

Tabla Factores y variables para probar la efectividad del diseño del modelo propuesto

Variable	Factor Relevante (indicador)	SI/NO	Peso (Madurez)
Perspectiva: Seguridad de la Información			
Políticas de seguridad de la información	Se declara con claridad la política		
	Se han definido los objetivos deseados de la política		
	Se establece los procedimientos de implementación de la política		
	Están definidos los roles y responsabilidades de acuerdo al MOF de Las Microfinancieras de Chiclayo		
	Se establece las sanciones de su incumplimiento		
	Se integra al Plan de Seguridad de la Información y de TI de Las Microfinancieras de Chiclayo		
	Se puede identificar las excepciones potenciales a las políticas de seguridad de información		
Perspectiva: Gestión de riesgos de TI			
Estructuración de la metodología de análisis y tratamiento de riesgos	Se ha definido nítidamente las categorías – como disponibilidad, integridad y confidencialidad – en las que se pueden agrupar los riesgos de TI		
	La gestión de riesgos de TI se integra en la gestión de riesgos general para todos los riesgos a nivel corporativo		
	Su estructura está diseñada para que los empleados relacionados con la gestión de la seguridad de TI y de riesgos puedan entenderlo		
Gobierno de los riesgos de TI	Contempla todas las variables necesarias exigidas por la SBS para su evaluación		
	Se ha establecido pautas para evaluar la magnitud de los riesgos		
	Se cuenta con indicadores clave para monitorizar periódicamente la eficacia de nuestras actividades de gestión de riesgos de TI		
Perspectiva: Continuidad de procesos			
Actividades básicas de continuidad de procesos	Identifica los procesos críticos de Las Microfinancieras de Chiclayo		
	Determina el RTO y RPO de cada proceso crítico		

Tabla: Factores y variables para probar la efectividad de la operación del modelo propuesto

Variable	Factor Relevante (indicador)	SI/NO	Peso (Madurez)
Perspectiva: Seguridad de la Información			
Políticas de seguridad de la información	A partir de las políticas de seguridad de la información definidas se puede normar y procedimentar los procesos de TI relacionados con la la seguridad de TI, gestión de riesgos de TI		
	A partir de las políticas de seguridad de la información definidas se pueden definir objetivos de control y controles relacionados con la seguridad de TI, gestión de riesgos de TI y continuidad de procesos		
	A partir de las políticas de seguridad de la información definidas se pueden definir indicadores clave para monitorizar periódicamente la eficacia de nuestras actividades de gestión de seguridad de TI, gestión de riesgos de TI		
Perspectiva: Gestión de riesgos de TI			
Análisis y tratamiento de riesgos	A partir del modelo propuestos se puede establecer un proceso formal y coherente para evaluar potenciales riesgos de TI		
	Se puede determinar con efectividad los niveles de riesgos inherentes de TI		
	Se puede evaluar la efectividad de los controles y hacer seguimiento de las brechas de seguridad		
Gobierno de los riesgos de TI	La información resultante del modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la gestión de riesgos de TI		
	La información resultante del modelo sirve para tomar deciciones con efectividad en relación a las inversiones e importancia de los controles de seguridad		
Perspectiva: Continuidad de procesos			
Gobierno de la continuidad de procesos de TI	La información resultante del modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la continuidad de procesos		
	A partir del modelo propuesto se puede establecer planes de contingencia y planes de mantenimiento de los activos críticos de TI		

ANEXO N° 02

RESULTADOS DEL ANÁLISIS DE RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMATICA

En el siguiente formato contiene el resumen del análisis y evaluación de los posibles riesgos relacionados con TI que afectan directamente los activos tecnológicos.

I. SERVIDORES Y CONCENTRADORES CENTRALES

Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Servidores y concentradores centrales y de borde	Acceso no autorizado	Si	Central (equipos centrales) El acceso a los recursos críticos en los gabinetes de piso o de pared (servidores, switch, router, modem, ups,) del cuarto de comunicaciones en las agencias está protegido con un sistema a los que sólo tiene acceso el personal autorizado.
		Parcialmente	En agencias (equipos de borde) Los gabinetes de comunicación están o disponibles ha ser abiertos o ubicados en un ambiente no apropiado, como almacén de productos de limpieza o compartiendo ambientes con la ventanilla de atención a clientes
	Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje	Si	Se cuenta con un sistema de red múltiple de alimentación de energía que evita el fallo de suministro. Así mismo, se cuenta con un sistema de alimentación ininterrumpido de energía para caso extremos de suministro de energía.
	Destrucción o fallo de un componente crítico del equipo (microprocesador, memoria, fuente de poder, otros)	Se recomienda mejorar	La seguridad para la entrada y salida de paquetes a Internet de todas las agencias está basada en un servidor ISA Server 2004 sin tolerancia a fallos por riesgos en fuente de poder, discos duros y procesador. No existen equipos de comunicación que toleren fallos este es el caso del switch core (aquí se conectan los servidores) ubicado en la oficina principal, y los switches ubicados en cada una de las agencias. Lo cual paralizaría las operaciones en todas las agencias en caso de avería.
	Errores de configuración	Se recomienda mejorar	Se cuenta con servidor de respaldo donde se replica toda la configuración necesaria para reiniciar el sistema. El servidor activo tiene implementado políticas de acceso a ser mejoradas, y no se cuenta con redundancia para este equipo altamente importante

	Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento racks, otros)	Debilidad en agencias	Se cuenta con sistema de aire acondicionado con BTU/h adecuado en el cuarto de comunicaciones de la oficina principal y en cada una de las agencias
	Límite de vida útil – Máquinas obsoletas (antigüedad del equipo, repotenciamiento de componentes)	Si	Se tiene pendiente un pedido para adquirir nuevos equipos centrales.
	Mal mantenimiento	Si	Hay un plan de mantenimiento de equipos.
	Robo	Si	Los equipos de cómputo están asegurados.
	Afectación por virus	Si	Protegidos con antivirus.

II. BASE DE DATOS

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Base de Datos	Copia no autorizada de o a un medio de datos externos	Si	Se generan backup diarios y son almacenados en DVD en bóveda, manejados y transportados por personal autorizado.
	Errores de software (motor y contenedor de base de datos)	Si	Se cuenta con servidor de respaldo donde se replica toda la configuración necesaria para reiniciar el sistema. El servidor activo tiene implementado políticas de acceso a ser mejoradas, y no se cuenta con redundancia para este equipo altamente importante.
	Falta de espacio de almacenamiento	Se recomienda mejorar	Se estima que en un tiempo próximo la arquitectura de datos con la que actualmente se trabaja no va a ser funcional y bajará su performance de respuesta
	Pérdida o falla de backups	Si	Se genera backup diarios de la base datos completa.
	Pérdida de confidencialidad en datos privados y de sistema	Se recomienda mejorar	El acceso a la base de datos está controlado a través de perfiles de usuario con niveles de acceso autorizados, según el área y responsabilidad.
	Directorios compartidos	Si	Directorio de la base de datos solo esta compartido para usuarios autorizados.
	Afectación de virus	Si	Servidor de base de datos protegido con antivirus

III. SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Sistemas operativos instalados en servidores y terminales	Aplicaciones sin licencias	Si	Software licenciado
	Error de configuración	Si	Software licenciado, con evaluación y pruebas.
	Mala Administración de control de accesos	Si	Se controla el acceso a las estaciones mediante política de acceso: niveles de acceso por perfiles de usuario.
	Pérdida de datos	Si	Mensualmente se generan backups.
	Afectación de virus	Si	Protegidos con antivirus

IV. BACKUP (SISTEMA DE RESPALDO)

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Backup	Copia no autorizada del backup	Si	Solo personal autorizado tiene acceso a generar, copiar y trasladar backup de información.
	Errores de software para recuperación de información de backup	Si	Su procedimiento de restore es copiando la última base de datos backup. Se instala, de ser necesario, toda la configuración mínima en los servidores.
	Falla o deterioro del medio de almacenamiento externo del backup	Si	Los backup son almacenados en dispositivos magnéticos (DVD), almacenados en bóveda.
	Falta de espacio de almacenamiento	Si	Backup tamaño 8 Gb 1.5 Gb en zip.
	Mala integridad de los datos al recuperar la información de un backup	Si	Los backups son revisados después de su grabación en los medios magnéticos
	Pérdida o robo de backups	Si	Solo personal autorizado tiene acceso a los backups
	Sabotaje	Si	Solo personal autorizado tiene acceso a los backups

V. CABLEADO Y CONCENTRADORES

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Cableado y concentradores	Conexión de cables inadmisible (modificación de conexiones y mal etiquetado)	Mejorar	Las malas condiciones del cableado para las redes informáticas, la ausencia de documentación de las pruebas de cableado y de los planos de distribución de cableado
	Factores ambientales	Mejorar	Se cuenta con sistema de aire acondicionado con BTU/h adecuado en el cuarto de comunicaciones de la oficina principal
	Accesos no autorizados.	Mejorar	Es posible conectar equipos portátiles en puntos de acceso a la red de datos sin que se genere un registro. Esto hace posible que intrusos puedan escanear y vulnerar a la red de datos de las agencias.
	Longitud de los cables de red excedidos a las normas	Si	Longitud de cables cumple con las normas establecidas.

VI. RED

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Red	Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)	Mejorar	Es posibles conectar equipos portátiles en puntos de acceso a la red de datos sin que se genere un registro. Esto hace posible que intrusos puedan escanear y vulnerar a la red de datos de las agencias.
	Configuración inadecuada de componentes de red	Si	Usuarios no pueden acceder a las configuraciones de red – acceso restringido
	Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros)	Mejorar	El ancho de banda asimétrico contratado a Telefónica resulta ser insuficiente para las 40 conexiones concurrentes a la base de datos que realizan en determinado momento las maquinas estaciones de trabajo en las diferentes agencias. Las pruebas demostraron que con 3 conexiones concurrentes prácticamente se satura el ancho de banda.
	Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)	Mejorar	Es posibles conectar equipos portátiles en puntos de acceso a la red de datos sin que se genere un registro. Esto hace posible que intrusos puedan escanear y vulnerar a la red de datos de las agencias.

VII. USUARIOS

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Usuarios	Acceso no autorizado a datos	Si	Cada usuario tiene un perfil y opciones asignadas para el acceso al sistema (Reporte de Perfiles – Opciones del Sistema Informático y Usuarios)
	Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida	Mejorar	Cada usuario cuenta con una clave personal, pero se comprobó que no existe una política adecuada para las contraseñas de los usuarios.
	Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)	Si	Local adecuado e instalaciones en todas las oficinas.
	Destrucción negligente de datos por parte de los usuarios	Si	Acceso a la base de datos protegido por password.
	Documentación deficiente (manual de usuario)	Mejorar	Se cuenta con manuales de usuario del sistema actualizados en 90 %.
	Entrada sin autorización a ambientes	Si	Solo personal autorizado tiene acceso a los ambientes de sistemas
	No cumplimiento con las medidas de seguridad del sistema	Si	Cada usuario tiene un perfil y opciones asignadas para el acceso al sistema y cada usuario cuenta con una clave personal intransferible

VIII. DOCUMENTACIÓN DEL SISTEMA

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Documentación de programas, hardware, procedimientos administrativos l, etc.	Acceso no autorizado a datos de documentación	Si	La documentación está en el Área de Tecnologías de Información sólo es accedida por personal autorizado.
	Borrado, modificación o revelación desautorizada de información	Si	La documentación es manipulada solo por el personal responsable.
	Copia no autorizada de un medio de documentación del sistema	Si	Sólo se proporciona copias de la documentación a personas autorizadas.
	Descripción de archivos y programas inadecuado	Mejorar	Se registran como "control de cambios". Falta implementar algunos formatos que se han definido en el PEI y PSI.
	Factores ambientales (almacén de documentación)	mejorar	La documentación está almacenada en medios magnéticos en instalaciones adecuadas.
	Mantenimiento y actualización inadecuado o ausente de la documentación	Si	Se actualiza la documentación cada vez que se hacen cambios en el sistema

IX. SISTEMA CONTABLE Y FINANCIERO

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
SIIF y SIG	Modificaciones inoportunas y no reglamentadas	Si	Se lleva el control detallado del desarrollo y mantenimiento por cada analista programador. "Control de cambios"
	Funcionalidad del sistema (no se atiende todos los requerimientos de los diferentes usuarios)	Si	Se reciben y analizan todos los requerimientos, los cuales son atendidos de acuerdo a su factibilidad y estimación de tiempos. (Prioridad Entidades Supervisoras – Negocios - Operaciones).
	Acceso a los programas fuentes no controlado	Si	Sólo el personal de la Sección de Desarrollo y Mantenimiento tiene acceso al código fuente del sistema informático.
	Validación en los procesos de captura y registro de transacciones	Mejorar	Existen observaciones de la SBS y de otras auditorias que indican falta de validación en algunos procesos.
	Sabotaje (eliminación de programas)	Si	Se maneja políticas de seguridad para los usuarios implementado en cada terminal.

ANEXO N° 04

TABLAS DE REFERENCIA PARA HALLAR LA VALORACIÓN DE LA CRITICIDAD DE LOS ACTIVOS DE TI

Para la valoración de los activos se tomarán en cuenta las siguientes dimensiones de seguridad:

Tabla de descripción de las dimensiones de seguridad de la información que se tomarán en cuenta en la valoración de la criticidad de los activos de TI

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Tabla de definición de escala de valoración de la criticidad de los activos de TI

Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1	pudiera causar molestias a un individuo
Obligaciones legales	
9	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	probablemente cause un incumplimiento grave de una ley o regulación
5	probablemente sea causa de incumplimiento de una ley o regulación
3	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	pudiera causar el incumplimiento leve o técnico de una ley o regulación
Seguridad	
9	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Intereses comerciales económicos	
9	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
5	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3	de bajo interés para la competencia de bajo valor comercial
1	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
de interrupción del servicio	
9	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3	Probablemente cause la interrupción de actividades propias de la Organización
1	Pudiera causar la interrupción de actividades propias de la Organización
de orden público	
9	alteración seria del orden público
7	probablemente cause manifestaciones, o presiones significativas
3	causa de protestas puntuales
1	pudiera causar protestas puntuales
operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	Probablemente merme la eficacia o seguridad de la misión operativa o logística
1	Pudiera mermar la eficacia o seguridad de la misión operativa o logística
administración y gestión	

9	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	probablemente impediría la operación efectiva de la Organización
5	probablemente impediría la operación efectiva de más de una parte de la Organización
3	probablemente impediría la operación efectiva de una parte de la Organización
1	pudiera impedir la operación efectiva de una parte de la Organización
pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
persecución de delitos	
6	Impida la investigación de delitos graves o facilite su comisión
1	Dificulte la investigación o facilite la comisión de delitos
tiempo de recuperación del servicio	
9	RTO < 4 horas
7	4 horas < RTO < 1 día
4	1 día < RTO < 5 días
1	5 días < RTO

ANEXO N° 06

CATÁLOGO DE VULNERABILIDADES POTENCIALES USADO EN EL MODELO DE GESTIÓN DE RIESGOS

N° Vulnerabilidad
1 Ausencia de personal
2 Acceso físico no autorizado
3 Acceso no autorizado a la documentación del sistema
4 Acceso no autorizado a la información
5 Acceso no autorizado a la información, redes y sistemas
6 Acceso no autorizado a las infraestructuras informáticas
7 Acceso no autorizado a las librerías fuente de los programas
8 Acceso no autorizado a los equipos de cómputo
9 Acceso no autorizado a redes y sus servicios
10 Acceso no autorizado al equipamiento informático
11 Acceso no autorizado, inadecuado o corrupción del soporte en el tránsito
12 Activos no protegidos
13 Atribución incorrecta de privilegios de acceso
14 Código malicioso
15 Complicated user interface
16 Confianza de las organizaciones clave hacia la compañía.
17 Conformidad con estándares
18 Conformidad con la política de seguridad
19 Control mal implantado
20 Coordinación de actividades de seguridad
21 Cumplimiento de las obligaciones y deberes del outsourcing (externalizació
22 Derecho a auditar en contratos de terceras partes
23 Derechos de propiedad intelectual
24 Disponibilidad de las infraestructuras de procesamiento de la información
25 Disposición o reutilización de los medios de almacenaje sin una apropiada verificación
26 Externalización y uso de terceras partes contratadas
27 Clima extremo
28 Fallo del sistema
29 Falta de un acuerdo de intercambio de software e información
30 Falta de coordinación y organización de la seguridad
31 Falta de planes y procedimientos de continuidad de negocio
32 Falta de política de seguridad
33 Falta de responsabilidades, pruebas y formación en la continuidad de negocio
34 Falta de seguridad en el equipamiento informático
35 Falta de seguridad en los soportes informáticos
36 Falta de sensibilización
37 Falta de una gestión apropiada de las claves criptográficas
38 Falta de una política determinada en el uso de controles criptográficos
39 Gestión de contraseñas que es demasiado simple
40 Manejo inadecuado de la red
41 Uso inadecuado o descuidado del control de acceso físico al edificio
42 Procedimientos inadecuados de reclutamiento

43 Respuesta inadecuada del servicio de mantenimiento
44 Uso Incorrecto del hardware y software
45 Incorrecta clasificación, etiquetado o manejo de la información.
46 Incumplimiento de la legislación
47 Insuficiente mantenimiento / mala instalación de los medios de almacenaje.
48 Entrenamiento insuficiente de seguridad
49 Insuficiente seguridad construida dentro del sistema
50 falta de seguimiento
51 Falta de copias back-up
52 Falta de cuidado en la disposición
53 Falta de documentación
54 Falta del control del cambio eficaz
55 Falta de control eficiente del cambio de configuración
56 Falta de mecanismos de identificación y de autentificación tales como autentificación de usuario
57 Falta de identificación y autentificación del remitente y del receptor
58 Falta de mecanismos de supervisión
59 Falta de esquemas de reemplazo periódicos
60 Falta de protección física del edificio, puertas y ventanas;
61 Falta de políticas para el uso correcto de los medios de telecomunicaciiones
62 Falta de pruebas de envío y recibimiento del mensaje
63 Falta del conocimiento sobre seguridad
64 Localización en un área susceptible a catástrofes
65 Nivel inapropiado de protección criptográfica
66 Dejar en sesión el sistema al salir del puesto de trabajo.
67 Prueba insuficiente del software
68 Pobre cableado
69 Administración pobre de contraseñas
70 Prevención del uso no autorizado de las infraestructuras de procesamiento
71 Procesamiento de negocio eficiente
72 Protección de datos y privacidad de la información personal
73 Protección de la información de la organización
74 Recolección de evidencias

ANEXO N° 07

EXIGENCIAS DE LA NORMA SBS CONSIDERADOS EN LOS ESTÁNDARES ISO/IEC 27001 Y MagerIT

Exigencia de la norma SBS		ISO/IEC 27001	MagerIT
Establecer e implementar políticas y procedimientos necesarios para administrar los riesgos de TI		X	
Cumplimiento de los criterios de control interno	Eficacia		
	Eficiencia		
	Confidencialidad		X
	Integridad		X
	Disponibilidad		X
	Cumplimiento normativo		
Definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información		X	
Mantener y documentar un sistema de administración de la seguridad de la información	Definición de una política de seguridad	X	
	Evaluación de riesgos de seguridad a los que está expuesta la información		X
	Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados		X
	Plan de implementación de los controles y procedimientos de revisión periódicos		X
	Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos		X
Responsabilidad de verificar que se mantengan las características de seguridad de la información en subcontrataciones	cumplimiento de la presente circular		
	los proveedores del servicio exterior, aseguran el adecuado acceso a la información con fines de supervisión		
Administración de la seguridad de la información	Seguridad lógica		
	Seguridad de personal		
	Seguridad física y ambiental		
	Clasificación de la seguridad		X
Administración de operaciones			
Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad			
Procedimientos de respaldo			
Planeamiento, criterios de diseño e implementación y pruebas		X	

de la continuidad de negocios		
Cumplimiento normativo	X	
Privacidad de la información	X	
Plan anual de trabajo para la evaluación de cumplimiento: Auditoría Interna y Externa	X	
Información a la Superintendencia	X	X
Sanciones en caso de incumplimiento	X	X

ANEXO N° 8
CUADRO COMPARATIVO ENTRE LA ISO/IEC 27001 Y EL MODELO PROPUESTO PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

Criterio		ISO/IEC 27001	Modelo Propuesto	Aporte de la investigación
Identifica los objetivos de negocio considerados en un sistema de seguridad de la información		Como norma internacional lo establece de carácter general como requisito de un sistema de seguridad de la información	Lo específica para el caso de estudio	Adecúa la norma al tipo de empresa
Selecciona del ámbito de implantación apropiado para la implantación de las políticas de seguridad de la información		Como norma internacional lo establece de carácter general como requisito de un sistema de seguridad de la información	Lo específica para los procesos críticos del caso de estudio	Adecúa la norma al tipo de empresa
Determina niveles de madurez de las políticas de seguridad de la información	Define documentos y formatos que especifique el ámbito de conformidad de la política	Lo define de manera general como requisito de un sistema de seguridad de la información	Si se ha considerado de manera específica para la evaluación de los controles actuales por activo de TI	Se ha diseñado formatos específicos para valorar las políticas y los controles
	Establece formas de inventario de activos de información	Lo define de manera general como requisito de un sistema de seguridad de la información	Si lo establece	Se ha normado una clasificación en la definición de la política relacionada con "Clasificación de activos"
	Clasifican los activos de información	No lo considera	Si lo establece	Se ha establecido una clasificación en la definición de la política relacionada con "Clasificación de activos"
	Define una lista de controles	No lo considera	Si lo establece	Se han identificado los controles específicos por cada activo en el caso de estudio
	Está establecido un proceso de gestión para la continuidad de negocio	Lo establece como un requisito de mejoramiento continuo (ciclo PDCA)	Si lo establece	Se ha elaborado un procedimiento para continuidad de procesos tomando como referencia las normas de la SBS y otras normas relacionadas con la continuidad de negocio
	Define programas de concienciación en seguridad	Lo define de manera general como requisito de un sistema de seguridad de la información	No lo establece	Se establece como recomendación
	Identifica	Lo establece	No lo establece	Se han establecido como

	acciones correctivas y preventivas	como un requisito de mejoramiento continuo	como un proceso, pero si como controles específicos	controles específicos
	Define mecanismos para medir la efectividad de los controles de las políticas de seguridad de la información	No define métricas, pero si establece que deben realizarse su seguimiento	No se ha definido métricas, pero si se ha considerado evaluación de brechas	Se considera un proceso de evaluación de brechas

ANEXO N° 9
CUADRO COMPARATIVO ENTRE LA MODELO MAGERIT Y EL MODELO PROPUESTO

CRITERIO	MODELO MAGERIT	MODELO PROPUESTO
Determinación de los activos de TI que requieren protección	Define un listado general clasificado por tipo de activo	Utiliza la propuesta de Magerit
Identificación de vulnerabilidades	No lo considera	Si lo considera
Identificación de amenazas	Define un listado general clasificado por tipo de activo	Utiliza la propuesta de Magerit
Estimación del impacto de las amenaza	Establece criterios de evaluación cuantitativa y cualitativa para el impacto de las amenazas	Sí se realiza
Estimación de la probabilidad de ocurrencia de las amenazas	Establece criterios de evaluación cuantitativa y cualitativa para la probabilidad de ocurrencia de las amenazas	Sí se realiza
Cálculo y clasificación del nivel de riesgo intrínseco	Determina una forma de valoración del riesgo intrínseco	Sí se realiza
Implementación de las medidas de seguridad	Determina de manera general formas de implementación de salvaguardas	Si se realiza
Identificación de la estrategia de implementación de controles	Determina de manera general las estrategias de implementación de controles	Sí se realiza
Cálculo y clasificación de la brecha de seguridad: nivel de riesgo residual	Determina una forma de valoración del riesgo residual	Sí se realiza
Evaluación del grado de madurez de los controles	No lo contempla	Sí se realiza