UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN ADMINISTRACIÓN FINANCIERA

"SISTEMA DE GESTIÓN DE RIESGOS DE ACTIVOS INFORMÁTICOS EN LAS MEDIANAS EMPRESAS FERRETERAS DE LA CIUDAD DE GUATEMALA, APLICANDO EL MARCO DE TRABAJO RISKIT"

ING. JORGE ALEJANDRO MEZA MORALES

GUATEMALA, NOVIEMBRE DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN ADMINISTRACIÓN FINANCIERA

"SISTEMA DE GESTIÓN DE RIESGOS DE ACTIVOS INFORMÁTICOS EN LAS MEDIANAS EMPRESAS FERRETERAS DE LA CIUDAD DE GUATEMALA, APLICANDO EL MARCO DE TRABAJO RISKIT"

Informe final de tesis para la obtención del Grado de Maestro en Ciencias, con base en el "Normativo de Tesis para Optar al Grado de Maestro en Ciencias", actualizado y aprobado por la Junta Directiva de la Facultad de Ciencias Económicas, en la resolución contenida en el Numeral 6.1, Punto SEXTO del Acta 15-2009 de la sesión celebrada el 14 de julio de 2009.

ASESOR:
LIC. MSc. JOSE RUBÉN RAMIREZ MOLINA

AUTOR:
ING. JORGE ALEJANDRO MEZA MORALES

GUATEMALA, NOVIEMBRE DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
HONORABLE JUNTA DIRECTIVA

Decano:	Lic. Luis Antonio Suárez Roldán
Secretario:	Lic. Carlos Roberto Cabrera Morales
Vocal Primero:	Lic. Carlos Alberto Hernández Gálvez
Vocal Segundo:	MSc. Byron Giovanni Mejía Victorio
Vocal Tercero:	Vacante
Vocal Cuarto:	P.C. Marlon Geovani Aquino Abdalla
Vocal Quinto:	P.C. Carlos Roberto Turcios Pérez

JURADO EXAMINADOR QUE PRACTICÓ EL EXAMEN PRIVADO DE TESIS
SEGÚN EL ACTA CORRESPONDIENTE

Presidente: MSc. Juan de Dios Alvarado López

Secretario: MSc. Edgar Enrique Abril Gálvez

Examinador: Dr. Edeliberto Cifuentes Medina

ACTA/EP No. 0208

ACTA No. 52-2017

En el Salón No. **3** del Edificio S-11 de la Escuela de Estudios de Postgrado, Facultad de Ciencias Económicas, Universidad de San Carlos de Guatemala, nos reunimos los infrascritos miembros del Jurado Examinador, el **14 de junio** de 2017, a las **18:00** horas para practicar el **EXAMEN GENERAL DE TESIS** del Ingeniero Electrónico **Jorge Alejandro Meza Morales,** carné No. **100020587**, estudiante de la Maestría en Administración Financiera de la Escuela de Estudios de Postgrado, como requisito para optar al grado de Maestro en Administración Financiera. El examen se realizó de acuerdo con el normativo de Tesis, aprobado por la Junta Directiva de la Facultad de Ciencias Económicas en el numeral 6.1, Punto SEXTO del Acta 15-2009 de la sesión celebrada el 14 de julio de 2009.----------

Cada examinador evaluó de manera oral los elementos técnico-formales y de contenido científico profesional del informe final presentado por el sustentante, denominado **"SISTEMA DE GESTIÓN DE RIESGOS DE ACTIVOS INFORMÁTICOS EN LAS MEDIANAS EMPRESAS FERRETERAS DE LA CIUDAD DE GUATEMALA, APLICANDO EL MARCO DE TRABAJO RISK IT"**, dejando constancia de lo actuado en las hojas de factores de evaluación proporcionadas por la Escuela. El examen fue **APROBADO** con una nota promedio de **71** puntos, obtenida de las calificaciones asignadas por cada integrante del jurado examinador. El Tribunal hace las siguientes recomendaciones: Que el sustentante incorpore las enmiendas señaladas dentro de los 45 días hábiles siguientes.

En fe de lo cual firmamos la presente acta en la Ciudad de Guatemala, a los catorce días del mes de junio del año dos mil diecisiete.

MSc. Juan de Dios Alvarado López
Presidente

MSc. Edgar Enrique Abril Gálvez
Secretario

MSc. Edeliberto Cifuentes Medina
Vocal I

Ing. Jorge Alejandro Meza Morales
Postulante

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO

ADENDUM

El infrascrito Presidente del Jurado Examinador CERTIFICA que el estudiante Jorge Alejandro Meza Morales, incorporó los cambios y enmiendas sugeridas por cada miembro examinador del Jurado.

Guatemala, 7 de agosto de 2017.

(f)_____

MSc. Juan de Dios Alvarado López
Presidente

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS
EDIFICIO "S-8"
Ciudad Universitaria zona 12
GUATEMALA, CENTROAMERICA

DECANATO DE LA FACULTAD DE CIENCIAS ECONÓMICAS GUATEMALA, DIEZ DE OCTUBRE DE DOS MIL DIECISIETE.

Con base en el Punto CUARTO, inciso 4.1 subinciso 4.1.2 del Acta 17-2017 de la sesión celebrada por la Junta Directiva de la Facultad el 27 de septiembre de 2017, se conoció el Acta Escuela de Estudios de Postgrado No. 52-2017 de aprobación del Examen Privado de Tesis, de fecha 14 de junio de 2017 y el trabajo de Tesis de Maestría en Administración Financiera: "SISTEMA DE GESTIÓN DE RIESGOS DE ACTIVOS INFORMÁTICOS EN LAS MEDIANAS EMPRESAS FERRETERAS DE LA CIUDAD DE GUATEMALA, APLICANDO EL MARCO DE TRABAJO RISK IT", que para su graduación profesional presentó el Ingeniero Electrónico **JORGE ALEJANDRO MEZA MORALES,** autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

LIC. LUIS ANTONIO SUÁREZ ROLDÁN
DECANO

M.CH

AGRADECIMIENTOS

A DIOS: por su obra en mi vida, dándome todo lo necesario para lograr esta meta. Le agradezco y le doy la gloria y la honra que merece por darme inteligencia, sabiduría, provisión, perseverancia, abundancia de tiempo y paciencia y sobre todo de su amor a lo largo de mi formación profesional.

A MIS PADRES: por haberme enseñado que es importante ser un hombre de bien e instruirme desde niño en los caminos de Dios nuestro Padre, logrando influenciar mi vida para que yo desee ser un hombre de bien para la sociedad.

A MI ESPOSA Y MI HIJO: Jessica y Jorge David, por ser parte de mi vida y servir de motor importante para desear ser mejor cada día. Por amarme, permitirme amarlos y estar conmigo en todo momento, sobre todo por apoyarme a lograr esta meta.

A MI HERMANA CRISTABELL: por haberme apoyado a lo largo de mi carrera atendiéndome y atendiendo a mis compañeros de universidad cuando llegábamos a estudiar y hacer tareas. Dios te bendiga por tu actitud de servicio y por honrarme con tu atención.

A MIS COMPAÑEROS DE CLASES: Jacky, Julio, Astrid, Héctor, Sergio y JC por haberme apoyado con las tareas, reuniones de estudio, ayudar a entender mejor los ejercicios de finanzas, contabilidad, para exámenes, momentos de diversión y platicas amenas que sin duda alguna siempre recordaré como una grata experiencia durante los años que convivimos como compañeros de clase.

A LOS CATEDRÁTICOS: Lic. Angel Mansilla, Lic. Edgar Guevara, Lic. Juan Carlos Sánchez, Lic. Erick Dardón, Lic. José Rubén Ramírez y Lic. Juan de Dios Alvarado por su excelencia para la cátedra, haciendo de mi desarrollo académico una grata y satisfactoria experiencia.

A LA ESCUELA DE ESTUDIOS DE POSTGRADO: por generar el ambiente y la posibilidad para que tuviera la oportunidad de optar al grado de maestro en ciencias en la disciplina de administración financiera.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: por estar al servicio de la sociedad guatemalteca, otorgando la oportunidad a los estudiantes de formarse y crecer profesionalmente para hacer de Guatemala un país mejor.

CONTENIDO

RESUMEN

En la ciudad de Guatemala, las medianas empresas ferreteras se dedican principalmente a la venta de distintos tipos de productos de manufactura extranjera, para proyectos relacionados con la construcción, decoración y remodelación; asimismo ofrecen distintos tipos de herramientas y materiales para actividades de carpintería, construcción, mecánica automotriz, pintura, electricidad, iluminación, cerrajería, plomería, entre otras.

Las ventas, cobros, determinación de costos de operación, que se realizan, se administran y controlan por medio de sistemas de información y/o por medio del apoyo de otro tipo de componentes tecnológicos a los cuales se les puede llamar también activos informáticos. Estos activos, son componentes que apoyan a la ejecución de procesos de negocio, los cuales deben funcionar en forma continua para no afectar la buena marcha de las empresas. El uso de tecnología en la ejecución de procesos de negocio involucra riesgos de interrupción, por lo que deben gestionarse adecuadamente para evitar o reducir pérdidas financieras y la creación de valor para los inversionistas.

El problema de investigación, en medianas empresas ferreteras de la ciudad de Guatemala, se refiere a que carecen de un adecuado sistema para la administración de riesgos de los activos informáticos, que permita prevenir o reducir pérdidas financieras por fallas o interrupciones en los procesos. Para el efecto, se presenta el Marco de Trabajo RISK IT (Riesgo de Tecnología de la Información), como una opción para que las empresas puedan administrar eficientemente los riesgos detectados y aplicar medidas adecuadas de mitigación.

El método científico fue la base de la metodología empleada para la realización de la presente investigación, siguiendo el proceso metodológico de investigación, con un enfoque cuantitativo, lo cual permitió la definición del problema, de los objetivos de investigación, construcción del marco teórico que sirvió de fundamento, formulación de la hipótesis, aplicación de técnicas de investigación de campo para

la recopilación de la información necesaria para la comprobación de la hipótesis y la presentación de las conclusiones de la investigación.

Los resultados más importantes y principales conclusiones de la investigación realizada determinaron que la gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información), en las medianas empresas ferreteras de la ciudad de Guatemala, integran la gestión de riesgos a la toma de decisiones y proveen de matrices de riesgo de activos informáticos, matrices de procesos de negocio, la ponderación de factores de riesgo para la creación de un mapa de apetito al riesgo de TI y la definición de un plan de mitigación de riesgos; asimismo, permite el análisis de impacto de pérdidas financieras por materialización de riesgos.

Los activos informáticos identificados de interés para la investigación fueron: Servidor 1, servidor 2, servicio de e-mail (correo electrónico), sistema de inventario y sistema de facturación. En los procesos de negocio se determinó que el riesgo de activos informáticos es crítico en el área de ventas, alto en inventarios, medio en tesorería y contabilidad y bajo en actividades de administración.

La proyección de pérdidas por materialización de riesgos de activos informáticos, en el año 2017, se cuantificó en GTQ 9,541,405 en el escenario optimista y GTQ.14,860,000 en el escenario pesimista. El impacto en cuentas del estado de resultados afecta ventas, inventarios y gastos de administración, proyectándose pérdidas de utilidad de GTQ 6,975,753 millones en el escenario optimista y de GTQ.10,500,000 millones en el escenario pesimista.

Luego de la definición de actividades de respuesta al riesgo, las pérdidas proyectadas en el año 2017, en el escenario optimista se reducen drásticamente a GTQ 2,805,551 y en el escenario pesimista a GTQ.4,505,000.

INTRODUCCIÓN

El sector de las medianas empresas ferreteras, en la ciudad de Guatemala, realiza un importante aporte a la actividad económica, al surtir a distintos tipos de empresas y personas particulares de diversidad de materiales y herramientas para la construcción, electricidad, carpintería, plomería, cerrajería, pintura, entre otros; asimismo, se enfocan en la mejora continua, y en prestar una adecuada atención personalizada y servicio al cliente. Las ferreterías se han modernizado desde sus inicios a finales del siglo XIX. Las más antiguas de la ciudad, son: ferretería El Globo, fundada en 1910, El Vapor y El Artesano, fundadas en 1935.

El sector de ferreterías medianas de la ciudad de Guatemala ha intensificado el uso de la tecnología de la información (TI) en la administración y ejecución de procesos de negocio, para el manejo de la cartera de clientes, ingresos y egresos de efectivo, ventas, compras, proveedores, costos y gastos de operación, inventarios, entre otros. El uso de la tecnología de la información aumenta la eficiencia de las empresas; sin embargo, implica riesgos operacionales relacionados con los activos informáticos, por falta de adecuación o fallas en los procesos internos, personal, fallas inesperadas en los sistemas, o bien la ocurrencia de eventos externos adversos.

El problema de la presente investigación financiera, se ha enfocado a la realización del diagnóstico de la situación de la administración de los riesgos de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala, y principalmente a la presentación de una propuesta para la aplicación del marco de trabajo RISK IT (Riesgo de Tecnología de la Información) para la adecuada seguridad y gestión de los riesgos de activos informáticos, basado en los conceptos de valor y beneficios, y el cumplimiento de los objetivos organizacionales.

La justificación de la presente investigación reside en la importancia que ha tomado el sector de medianas empresas de ferretería en la ciudad de Guatemala, en vista de que estas empresas privadas se encargan de la generación de fuentes de empleo, crean riqueza para sus inversionistas, contribuyen con el pago de impuestos para que el Estado pueda cumplir sus fines de bienestar social, proveen a sus clientes de diversos tipos de materiales y productos para distintas actividades económicas productivas, y para uso en el hogar; además, se justifica la necesidad de que el sector objeto de estudio haga una adecuada gestión de riesgos de sus activos informáticos para prevenir y mitigar fallas que puedan afectar su funcionamiento normal como empresa y la adecuada atención a sus clientes, proveedores y público en general.

El objetivo general de la presente investigación, es el siguiente: Desarrollar un sistema de gestión de riesgo de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala, con base en el marco de trabajo RISK IT (Riesgo de Tecnología de la Información), para integrar la gestión de riesgos a la toma de decisiones, con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo, la tolerancia al riesgo y la respuesta de la organización a los riesgos.

Los objetivos específicos, son Diseñar un modelo para la recolección de datos de los riesgos de los activos informáticos y la tecnología de la información utilizada para los negocios, incluyendo el entorno operativo, eventos de riesgo y factores de riesgo, para la construcción de la matriz de riesgos de activos informáticos, la matriz de procesos de negocio y la ponderación de factores de riesgo; desarrollar la matriz de evaluación de riesgos de tecnología de la información (TI), con base en el modelo RACI (por sus siglas en inglés, de Responsible, accountable, consulted, e informed) que corresponde a: Responsable, rendidor de cuentas, consultado e informado, como base para la rendición de cuentas de los que deben velar por que las actividades se realicen con éxito; analizar los resultados de la matriz de evaluación de riesgos de activos informáticos, con base en el análisis de procesos, frecuencia de ocurrencia e impacto financiero, para establecer la escala

de impacto financiero, en categorías y en unidades monetarias; crear el mapa de apetito de riesgo de TI, con base en la matriz de evaluación de riesgos, como herramienta visual para determinar el nivel de importancia en cuatro bandas: Rojo, riesgo inaceptable; amarillo, riesgo elevado; verde, nivel aceptable o normal de riesgo; y, azul, riesgo muy bajo; definir un plan de mitigación de riesgos de activos informáticos con base en el marco de trabajo RISK IT con el fin de priorizar riesgos y analizar el impacto financiero de su ocurrencia tomando en cuenta escenarios optimista y pesimista; elaborar el estado de resultados pro forma base, y de los escenarios optimista y pesimista, para analizar el impacto de pérdidas en ventas, inventarios, gastos de administración y pérdida total; definir actividades de mitigación para la respuesta a los riesgos de activos informáticos catalogados en un nivel de riesgo inaceptable, para analizar impacto financiero y la gestión de riesgo post mitigación.

La hipótesis de investigación formulada como respuesta tentativa al problema, es la siguiente. El diseño e implementación de un sistema de gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información), en las medianas empresas ferreteras de la ciudad de Guatemala, permite integrar la gestión de riesgos a la toma de decisiones; la construcción de la matriz de riesgo de activos informáticos, la matriz de procesos de negocio y la ponderación de factores de riesgo; la creación del mapa de apetito al riesgo de TI; la definición de un plan de mitigación de riesgos; el análisis del impacto en pérdidas financieras; el análisis de escenarios optimista y pesimista; y, la definición de actividades de mitigación para la respuesta a los riesgos de activos informáticos catalogados en un nivel inaceptable y estrictamente inaceptable.

El presente informe de tesis, consta de los siguientes capítulos: El capítulo Uno, expone los antecedentes sobre el sector de ferreterías en la ciudad de Guatemala, del riesgo de tecnología de la información (TI), de la gestión de riesgos de tecnología de la información (TI) y de la Asociación de Auditoría y Control de

Sistemas de Información de ahora en adelante (ISACA, por sus siglas en inglés, Information Systems Audit and Control Association).

El capítulo Dos contiene el marco teórico que fundamenta la investigación, relacionado con el riesgo, gestión y medición del nivel de riesgo, gestión de riesgo de tecnología de la información (TI), Marco de trabajo RISK IT para la gestión de riesgo de tecnología de la información, administración financiera, estados financieros, estados pro forma y el proceso de desarrollo del caso de negocio.

El capítulo Tres presenta la metodología de investigación que explica en detalle qué y cómo se hizo para resolver el problema de la investigación y presenta el resumen del proceso de investigación realizado

El capítulo Cuatro, contiene el modelo de recolección de datos de riesgos de tecnología de la información (TI), de las matrices de activos informáticos, de procesos de negocio y de riesgos de tecnología de la información (TI).

El capítulo Cinco, expone el desarrollo del Marco de Trabajo RISK IT (riesgo de tecnología de la información), para la gestión de riesgos de activos informáticos en medianas empresas ferreteras de la ciudad de Guatemala, incluyendo el análisis en la matriz de riesgo de activos informáticos, la elaboración del mapa de apetito de riesgo, el plan de mitigación de riesgos de activos informáticos, proyecciones de pérdidas por materialización de riesgos, estados de resultados pro forma, análisis de escenarios y el análisis financiero de las actividades de respuesta al riesgo. El capítulo Seis, presenta los resultados de la gestión de riesgos de activos informáticos, post mitigación.

Finalmente se presentan las conclusiones y recomendaciones de la investigación realizada.

1. ANTECEDENTES

Los antecedentes constituyen el origen del trabajo de investigación, indicando el marco de referencia teórico y empírico que relaciona a las ferreterías medianas de la ciudad de Guatemala con la gestión de riesgo de los activos informáticos.

1.1 Antecedentes de las ferreterías en la ciudad de Guatemala

De acuerdo con investigación del Diario de Centro América (DCA 2012), las primeras ferreterías de la ciudad Capital, se ubicaron en la zona 1, principalmente en la Cuarta Avenida.

La más antigua es Ferretería El Globo, que abrió sus puertas en el mercado guatemalteco en el año 1910, comercializando a la fecha productos de marcas tales como Stanley, Irwin Tools, Yale, Sika, Eastman, Victorinox, Pferd, Bosch, Cuprum, entre otras. (DCA 2012).

Ferretería El Vapor, fundada en 1935, ofrece productos para carpintería, cerrajería, construcción e industria, electricidad, herrajes, herramientas eléctricas, jardinería, puntura, plomería, entre otros. Ferretería El Artesano, también fue fundada en 1935. Ferretería Lewonski, fundada en 1955, ofrece productos que en su mayoría provienen de importaciones directas de Europa, Norte América, Asia, África y Sur. Ferretería El Tejar, 1951, Ferretería La Llave, fue fundada en el año 1961. (DCA 2012).

Antillon, fue fundada en 1952, iniciando con la venta de electrodomésticos, pero con el transcurso del tiempo se ha especializado en la venta de materiales eléctricos. Lo mismo sucede con CELASA, que inició operaciones en 1957 que se especializa en la venta de cables, alambres, iluminación, led, paneles solares, calentadores solares, transformadores, tubería, canaleta, tableros, entre otros.

Instalaciones Modernas, fue fundada en 1968 y a la fecha ofrece productos de grifería, calentadores, lavatrastos, loza sanitaria, entre otros. Las ferreterías más

antiguas, El Globo, El Vapor, Lewonski, La Llave, continúan operado; asimismo, se han agregado al mercado otras ferreterías, tales como, Super Mayen, Cefesa, Multimateriales, El Trébol, El Elefante, El Pacífico, entre otras.

Existen también grandes ferreterías, tales como CEMACO, NOVEX, EPA, y FFACSA, EL ARENAL, que cuentan con cadenas de tiendas, están enfocadas hacia el servicio al cliente, y se organizan por departamentos de blancos y baños, cocina y electrodomésticos, ferretería, organización, limpieza, jardinería y terraza, materiales de construcción, pintura, eléctricos; además, ofrecen distintos tipos de servicios tales como instalación de cerraduras, despacho a domicilio, compra desde su propio vehículo, compra en línea, cortes de madera a la medida, entre otros.

1.2 Antecedentes del riesgo de tecnología de la información (TI)

De acuerdo con Gallegos (2015), la alta tecnificación de las empresas modernas, la hace vulnerables a los riesgos de TI. El desafío es que, en vez de tratar de evitar los riesgos relativos a la tecnología, las empresas en mayor o menor medida, están aprendiendo a manejarlos para que el negocio avance, apoyándose en innovaciones estratégicas en materia de seguridad. Esto no implica solamente hardware y software sino también planes de concienciación en materia de seguridad. Para las amenazas detectadas en un análisis de riesgos que se realizan, se diseñan planes de acción para su mitigación parcial o completa. Una amenaza que se materializa constituye, en la mayoría de los casos, un riesgo operacional, dado que dicha materialización supone una pérdida económica para la organización. Para el riesgo de TI, la siguiente fórmula analiza el nivel de cobertura que posee una compañía: Riesgo residual = riesgo inherente – opciones de mitigación.

El riesgo inherente es el riesgo latente que toda empresa tiene: es la amenaza en su estado más puro y potenciado. Los mitigantes son las acciones que la

organización decide realizar para contrarrestar el riesgo inherente, ya sea tomando acciones orientadas a reducirlo (el riesgo no desaparece se atenúa), de transferencia (las acciones para combatir las amenazas son transferidas a otra empresa), asumir el riesgo aceptando la amenaza (riesgo asumido, que es muy diferente al riesgo no identificado) o bien la máxima, que es la remediación total. (Gallegos 2015).

La organización es responsable de fijar el nivel de “apetito al riesgo”, lo cual es una declaración implícita del nivel de riesgo que está dispuesta a asumir. Esta situación es aún más crítica cuando la empresa está sujeta a inspecciones de entes reguladores, como es el caso de las entidades financieras. Al respecto, el Comité de Basilea define el riesgo operacional como el riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas, o bien de aquellas que sean producto de eventos externos. Es decir, que es el riesgo en el que incurre una empresa por su operación, que no está clasificado como riesgo de crédito o de mercado, o los otros tradicionales, y que ha cobrado gran notoriedad dada la mayor participación de operaciones tercerizadas, sistemas tecnológicos complejos, productos derivados y estructurados, y una mayor diversidad de negocios financieros. (Gallegos 2015).

Un adecuado proceso de gestión del riesgo operacional, se refiere a la identificación, evaluación, seguimiento, control y mitigación del riesgo operacional. Estos cuatro elementos reflejan el enfoque principal de la gestión de riesgos presente en todos los documentos y mejores prácticas del Comité de Basilea y, por ende, en las normativas sobre riesgo operacional de todos los países avanzados del mundo. (Gallegos 2015).

Integrado el riesgo de TI, con el riesgo operacional, se puede mencionar que por definición, el riesgo operacional recoge la pérdida potencial derivada de deficiencias significativas en la integridad o confianza del sistema, pudiendo surgir

de un mal uso del cliente, un diseño inadecuado de un sistema o bien un sistema mal implantado. Es decir, que el riesgo operacional se encuentra en estrecha relación con los riesgos de TI. Cuando se realiza un análisis de riesgo de TI se detectan distintos tipos de amenazas que están relacionadas usualmente a: (Gallegos 2015).

- Instalaciones
- Proveedores
- Recursos humanos clave
- Telecomunicaciones
- Hardware
- Sistemas operativos
- Aplicaciones

Para contrarrestar las amenazas detectadas, es importante tomar acciones a fin de eliminarlas o bien minimizar el impacto si estas se produjeran. De acuerdo con el estándar internacional COBIT (Control Objectives for Information and related Technology), una buena práctica para el control de la información TI y la elaboración de un marco de trabajo para efectuar el análisis de riesgos de los activos informáticos, requiere la consideración de las siguientes entradas: (Gallegos 2015).

- Definición de planes estratégicos y tácticos de TI.
- Plan de administración de proyectos.
- Administración de servicios de terceros.

- Continuidad de servicio (BIA).
- Seguridad de los sistemas.
- Monitoreo y evaluación del desempeño de TI.
- Gobierno de TI.

1.3 Antecedentes de la gestión de riesgos de tecnología de la información (TI)

Según lo expone Treviño (2009, los conceptos tradicionales de riesgo, auditoría y control han evolucionado hacia conceptos más amplios como el Corporate Governance (Gobierno Corporativo) y el IT Governance (Gobierno de TI), como resultado de las estrictas regulaciones sobre el control interno, el riesgo operacional, las responsabilidades de la alta Gerencia y la necesidad de alinear la TI con la estrategia del negocio.

El Gobierno Corporativo refiere a cómo una organización, a través de varios roles y responsabilidades de sus Directores y de la propia Administración: (Treviño 2009).

- Fija los objetivos corporativos
- Ejecuta las operaciones diarias del negocio
- Monitorea el desempeño de la organización y su personal
- Integra a sus stakeholders
- Alinea el comportamiento y las actividades corporativas
- Cumple con leyes y regulaciones aplicables

El Gobierno TI, parte integral del Gobierno Corporativo, contempla el liderazgo, estructuras de organización y procesos que aseguran que la Tecnología de la Información, soporta los objetivos y estrategias de la organización. (Treviño 2009). En el riesgo asociado a la TI es común observar, entre otros, los siguientes hechos:

- La TI sigue expuesta a riesgos relacionados con la seguridad de sus sistemas, la continuidad del servicio, los fraudes, daños en la infraestructura, pérdidas o alteraciones de información sensible, multas o penalizaciones, incidentes operativos, daños físicos y ambientales.

- Los sistemas aplicativos y su infraestructura, no cubren las expectativas para el negocio o simplemente son desaprovechados.

- Ausencia de Gobierno de TI: Las prácticas de operación y control de la TI son informales, existen muchos re-trabajos, tiempos elevados para realizar mantenimientos de aplicaciones, cuellos de botella en proyectos, niveles bajos de calidad en el servicio, deficiente organización de las actividades internas.

- El área encargada de TI es vista como un área de “gasto permanente” y no se muestra aún ningún retorno a la inversión.

Para la creación de un marco de riesgo, ha sido necesario: (Treviño 2009).

- Reconocer la existencia de riesgos de TI

- Identificación, evaluación y administración de riesgos.

- Reconocer que existe dependencia muy importante del negocio, hacia el funcionamiento continuo de la TI y por ende hacia el manejo de sus riesgos.

El Marco de Riesgos de TI (The Risk IT Framework) es producto de la investigación y aporte de la experiencia conjunta de un equipo global de especialistas, para a la alta Gerencia, una administración efectiva de los riesgos de TI relacionados con el negocio, a partir de su identificación y evaluación. Este marco representa el eslabón entre el ERM (Enterprise Risk Management) y el IT Risk Management, cubriendo además en su totalidad el Marco IT Governance. Asimismo, este marco se constituyó a partir de los componentes de riesgo relacionados dentro de los marcos de COBIT y Val IT. (Treviño 2009).

El riesgo de TI es el riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI dentro de la empresa. Este riesgo consiste en los eventos relacionados con la TI que pueden potencialmente impactar al negocio. Cada evento puede ser visto como Riesgo y Oportunidad. (Treviño 2009).

El riesgo de TI, se refiere a lo siguiente: (Treviño 2009).

- Eventos adversos relacionados con TI que destruyen valor.
- Valor de negocio no realizado o reducido a través de la TI.
- Oportunidades omitidas de asistencia de TI.

La oportunidad de TI, consiste en: (Treviño 2009).

- Identificación de nuevas oportunidades de negocio a través del uso de la TI.
- Incremento del valor del negocio a través del uso óptimo de las capacidades de TI.

1.4 Asociación de Auditoría y Control de Sistemas de Información de ahora en adelante (ISACA, por sus siglas en inglés, Information Systems Audit and Control Association)

En 1967 se creó la Asociación de Auditoría y Control de Sistemas de Información de ahora en adelante (ISACA, por sus siglas en inglés, Information Systems Audit and Control Association), la cual ha generado varios marcos de trabajo que apoyan a las organizaciones a alcanzar sus objetivos estratégicos, definiendo lineamientos como buenas prácticas de industria en materia de tecnología de la información. Entre los marcos de trabajo que han creado están los siguientes:

1.4.1 VAL IT

Val IT busca generar la relación adecuada entre la organización estratégica y la organización de TI de las empresas para lograr obtener el máximo valor de las inversiones en tecnología de la información y la gestión del portafolio de proyectos de tecnología de la información. El objetivo primordial de VAL IT es alinear las inversiones y los proyectos de la tecnología de la información a los objetivos estratégicos de las empresas, para apoyarles a alcanzarlos. ISACA (2009:11)

1.4.2 COBIT (Control Objectives for Information and related Technology)

El objetivo de COBIT es gobernar los procesos que tienen relación a eventos internos o externos de la tecnología de la información. Se enfoca eventos como incidentes operacionales, proyectos no alcanzados, cambios en los planes estratégicos de la tecnología de la información, etc. Busca también preparar a las empresas para factores externos como cambios en los mercados, nuevos competidores, nuevas tecnologías, cambios en regulaciones, así como nuevas regulaciones. Se encarga de gestionar todas las actividades relacionadas con TI en la organización. Estos procesos tienen que tratar con eventos internos o externos a la organización. Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las

fusiones. Los eventos externos pueden incluir cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y las nuevas regulaciones que le afectan.

Existen otros marcos de trabajo relevantes que fueron creados por la Asociación de Auditoría y Control de Sistemas de Información (de ahora en adelante ISACA), los cuales son interesantes, pero para esta investigación el más relevante, además de VAL IT y COBIT es RISK IT.

1.5 Marco de trabajo RISK IT

A continuación, presenta una reseña histórica del marco de trabajo RISK IT publicada en el sitio Web de ISACA: Para proporcionar a las Organizaciones de todo el mundo de una visión de los riesgos asociados a las iniciativas de TI, ISACA ha desarrollado la edición en Español del Marco de Riesgos de TI: partiendo como base del COBIT, ISACA reconocida mundialmente por su desarrollo del Marco de Buen Gobierno TI COBIT, proporciona el “eslabón perdido” entre la convencional gestión de riesgos empresariales y la gestión de riesgos de TI y el control. Las Organizaciones logran beneficios al aceptar sus riesgos, sin embargo, cuando sus riesgos son mitigados son inducidas para lograr mayores beneficios de forma sostenible. ISACA (2009:11).

ISACA, una asociación sin ánimo de lucro que cuenta con más de 86,000 profesionales de las Tecnologías de la Información (TI), ha desarrollado en el 2009, el Marco de Riesgos de TI en respuesta a la demanda de sus miembros y la industria. El marco y los documentos de apoyo son el resultado de miles de horas de trabajo de un equipo de expertos en TI y en los negocios, y de 60 revisores expertos de todo el mundo.

El Marco de Riesgos de TI reduce costes, esfuerzo y tiempo proporcionando una metodología clara enfocada en los riesgos de los negocios basada en TI como la finalización tardía de proyectos, cumplimiento normativo y legal, des alineamiento,

arquitectura obsoleta de TI, problemas en la entrega de servicios. Provee una guía para los ejecutivos y gestores a centrarse en las preguntas clave, tomar mejores decisiones ajustadas a sus riesgos y dirigir sus organizaciones a gestionar los riesgos de forma eficiente. Ofrece una visión única y completa de los riesgos de los negocios basada en TI, que costarán a las organizaciones millones al año por la pérdida de ingresos y oportunidades. ISACA (2009:11).

Riesgo y Valor son dos caras de la misma moneda. El Riesgo es inherente a todas las Organizaciones, debemos lograr un equilibrio que evite la destrucción del valor y asegurarnos que las oportunidades de creación de valor no se pierdan. Es importante ayudar a todos los niveles de la organización a gestionar los riesgos para obtener mayores beneficios y ayuda a detectar anticipadamente las señales de alerta. ISACA (2009:11).

El Marco de Riesgos TI complementa y extiende COBIT y Val IT, siendo muy eficaz como marco independiente. Un aspecto clave para todas las organizaciones que utilicen TI, desde empresas unipersonales hasta consorcios multinacionales, es que pueden obtener beneficios y ventajas de Marco de Riesgos TI. También es posible que se adopte por cualquier tipo de empresa en cualquier ubicación geográfica.” ISACA (2009:11).

2. MARCO TEÓRICO

El marco teórico expone las teorías y enfoques de análisis conceptuales que se utilizaron como fundamento de la investigación relacionada con la gestión de riesgo de los activos informáticos en medianas empresas ferreteras de la ciudad de Guatemala.

2.1 Tecnología de la información (TI)

De acuerdo con Guitert y Barajas (2004), con el nombre de tecnologías de la información, TI, se conoce al conjunto de tecnologías que permiten la adquisición, la producción, el almacenamiento, el procesamiento y la transmisión de datos y otras informaciones por medio de señales de naturaleza acústica, óptica o electromagnética. Teniendo en cuenta estas consideraciones, las tecnologías de la información y la comunicación engloban la microelectrónica, la informática y las telecomunicaciones.

Según Romero et al. (2014), las tecnologías de la información y la comunicación (TIC) son un conjunto de técnicas, desarrollos y dispositivos avanzados, que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos, siendo sus principales características: Son de carácter innovador y creativo, pues dan acceso a nuevas formas de comunicación y tienen mayor influencia y benefician en mayor proporción al área educativa, puesto que la hace más accesible dinámica.

Las tecnologías de información son herramientas que se agregan en las finanzas, la contabilidad, los recursos humanos, la logística y las operaciones. Comprenderlas y usarlas es un componente vital en el éxito de los negocios y organizaciones. (Cohen y Asís 2009). Los sistemas de información (SI) han venido a cambiar la forma en que operan las organizaciones. A partir de su uso se logran importantes mejoras, como la automatización de los procesos operativos que

proporcionan información de apoyo al proceso de toma de decisiones y, lo que es más importante, su implantación facilita el logro de ventajas competitivas.

De modo que la aplicación de las tecnologías de información en los negocios constituye un campo de estudio fundamental para la ciencia de la administración y gestión de negocios. Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware). Sin embargo, en la práctica se utiliza como sinónimo de “sistema de información computarizado”. Estos elementos son de naturaleza diversa e incluyen: (Cohen y Asís 2009).

- El equipo computacional: es el hardware necesario para que el sistema de información opere. Lo constituyen las computadoras y el equipo periférico.
- El recurso humano que interactúa con el sistema de información: las personas que utilizan el sistema, lo alimentan con datos o utilizan los resultados que genera.
- Los datos o información fuente: son todas las entradas que el sistema necesita para generar la información que se desea.
- Los programas que ejecuta la computadora y que producen diferentes tipos de resultados: los programas procesan los datos de entrada y generan los resultados que se esperan.
- Las telecomunicaciones: básicamente el hardware y el software que transmiten en forma electrónica texto, datos, imágenes y voz.
- Procedimientos: que incluyen las políticas y reglas de operación, tanto en la parte funcional del proceso de negocio, como los mecanismos para hacer trabajar una aplicación en la computadora.

El término tecnologías de información (TI), en inglés IT (Information technology), hace referencia a todas aquellas tecnologías que permiten y dan soporte a la construcción y operación de los sistemas de información, y son tecnologías de hardware, software, de almacenamiento y de comunicaciones. Estas tecnologías forman la infraestructura tecnológica de la empresa, que provee una plataforma en la cual la compañía construye y opera los sistemas de información. A continuación se presenta una lista no exhaustiva de estas tecnologías, algunas de las cuales serán comentadas a lo largo de este texto: redes de datos, redes de voz, satélites, sistemas de telefonía, medios de transmisión como fibra óptica, redes inalámbricas, "ruteadores" (routers), concentradores (hubs), módems, reproductores de discos compactos (CD-ROM, DVD-ROM), sistemas operativos, protocolos de comunicación y otros sistemas de almacenamiento. (Cohen y Asís 2009).

2.2 Riesgo

Según la Oficina de las Naciones Unidas para la Reducción de Desastres (UNISDR, The United Nations Office for Disaster Risk Reduction por sus siglas en inglés), riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. Oficina de las Naciones Unidas para la Reducción de Desastres (2004:1). Los riesgos pueden reducirse, manejarse, trasladarse, compartirse, evitarse, pero jamás eliminarse.

2.2.1 Gestión de riesgos

De acuerdo con INCIBE (2017), la gestión de riesgos está presente, con mayor o menor protagonismo, en distintos ámbitos de la sociedad y la empresa. Son algunos ejemplos la gestión de riesgos:

- Laborales
- Alimentarios
- Bancarios, financieros
- Corporativos
- De proyectos
- Medioambientales
- De seguridad de la información

Un hecho común a todos ellos, es que los responsables son conscientes de la existencia de amenazas que suponen un peligro para la consecución de sus objetivos. Dedican esfuerzos y recursos a mantener estos riesgos por debajo de un límite previamente consensuado en sus organizaciones. Para maximizar los beneficios de dicha gestión y contar con garantías de éxito, los esfuerzos han de ser empleados de forma metódica, estructurada y, sobre todo, siguiendo un proceso de evaluación y mejora continua. Las organizaciones se encuentran en un entorno en cambio constante. Los logros obtenidos ante las amenazas de hoy no suponen ninguna garantía de éxito para las amenazas de mañana. (INCIBE 2017). Algunos conceptos relacionados con la gestión de riesgos, son los siguientes:

- **Activo**

Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo. Este término se generaliza para

denominarse “fuente de riesgo”, siendo el elemento que sólo o con otros puede originar un riesgo.

- **Amenaza**

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Este concepto se amplia para denominarse “suceso”.

- **Vulnerabilidad**

Debilidad que presentan los activos y que facilita la materialización de las amenazas.

- **Impacto o consecuencia de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad**

El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo. La consecuencia es el resultado de un suceso que afecta a los objetivos.

- **Probabilidad**

Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos). Este término permanece en evolución de las normas ISO, refiriéndose a un suceso en lugar de a una amenaza.

Los principios básicos que debe cumplir la gestión de riesgos para que cumpla su cometido, son los siguientes:

- Proteger el valor, es decir, contribuir a la consecución de los objetivos y la mejora del desempeño
- Ser una parte integral de todos los procesos de la empresa
- Formar parte de la toma de decisiones
- Tratar explícitamente la incertidumbre
- Ser sistemática, estructurada y oportuna
- Basarse en la mejor información disponible
- Adaptarse, alineándose con el contexto interno y externo y con los perfiles del riesgo
- Integrar factores humanos y culturales
- Ser trasparente y participativa
- Ser dinámica, iterativa y responde a los cambios
- Facilitar la mejora continua

2.2.2 Medición del nivel de riesgo

El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma. (INCIBE 2017).

El impacto, y por tanto el riesgo, se valoran en términos del coste derivado del valor de los activos afectados considerando, además de los daños producidos en el propio activo:

- Daños personales

- Pérdidas financieras
- Interrupción del servicio
- Pérdida de imagen y reputación
- Disminución del rendimiento

Si bien es posible, y en ocasiones necesario, realizar un análisis cualitativo, trabajar con magnitudes económicas facilita a las organizaciones establecer el llamado umbral de riesgo, también llamado “apetito al riesgo”: el nivel máximo de riesgo que la empresa está dispuesta o “se atreve” a soportar. La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral. Por otro lado, se denomina coste de protección al coste que supone para las organizaciones los recursos y esfuerzos que dedican para mantener el nivel de riesgo por debajo del umbral deseado. Las organizaciones deben vigilar de no emplear más recursos de los necesarios para cumplir ese objetivo. El punto en el que el coste de protección es el adecuado para mantener los riesgos por debajo del umbral fijado de riesgo es el coste de equilibrio. Este punto dependerá del umbral de riesgo de acuerdo con los objetivos de la empresa.

2.2.3 Marco de trabajo

Como en toda actividad, el compromiso de la dirección es básico para llevarla a cabo con éxito. En la gestión de riesgos no es diferente, ha de estar plenamente integrada en los procesos de la empresa y requiere un compromiso fuerte y sostenido de la dirección así como del establecimiento de una rigurosa planificación estratégica, un marco de trabajo. Este “marco de trabajo” ha de ser objeto de seguimiento y revisión periódica que permitan medir el progreso y adaptarse a los cambios del entorno, tomando las decisiones oportunas para la mejora continua. (INCIBE 2017). Para conseguir una buena gestión del riesgo el marco de trabajo definido ha de:

- Comprender la empresa y su contexto
- Establecer una política de gestión de riesgos
- Identificar autoridades y competencias
- Definir la integración en los procesos de negocio como plan estratégico para que sea relevante, eficaz y eficiente
- Proporcionar los recursos necesarios: personas, formación, procesos y procedimientos, métodos y herramientas
- Establecer mecanismos de comunicación interna y externa

2.3 Gestión de riesgo de tecnología de la información (TI)

La gestión de riesgos de tecnología de la información se define acorde al programa de auditoría y asesoría de gestión de riesgos de la tecnología de la información, publicado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés, Information Systems Audit and Control Association).

El riesgo de tecnología de la información es una componente del universo de riesgo total de una organización. Las tecnologías de información y los sistemas son una parte mayo de la infraestructura de las organizaciones. La integración y alineamiento del riesgo de la tecnología y el riesgo empresarial o riesgo de negocio es necesario. El riesgo de tecnología de la información es específicamente riesgo de negocio, específicamente, riesgo de negocio asociado con el uso, propiedad, operación, participación, influencia y adopción de la tecnología de la información en una empresa. Consiste en eventos relacionados a la tecnología de la información y condiciones que pueden potencialmente impactar al negocio, por lo que es necesario reaccionar ante tales riesgos. ISACA (2012:11)

El objetivo primario de la tecnología de la información es el de la entrega de servicios para las operaciones de negocio. En esta capacidad, el riesgo de la tecnología de la información tiene incidencia en la habilidad de la tecnología de la información para entregar servicios que le permitan a las empresas llevar a cabo sus actividades operacionales diarias. Sin embargo, la gestión de riesgo de tecnología de la información también se enfoca en el desarrollo, adquisición y mantenimiento de procesos. Esto se relaciona directamente con asegurar el correcto desarrollo y mantenimiento de procesos de negocio que operan para generar rentabilidad, así como atender necesidades de negocio en una manera efectiva. Finalmente, la gestión de riesgos de tecnología de la información, se enfoca en proveer valor y/o beneficios a las empresas a través de la automatización. ISACA (2009:11)

2.3.1 Marco de trabajo riesgos de tecnología de la información

ISACA es la institución más reconocida a nivel mundial en materia de Auditoría y Control de sistemas de información. Debido a esto, se selecciona el marco de trabajo de Riesgos de la tecnología de la información. En los documentos publicados por ISACA para el marco de trabajo de Riesgos de la tecnología de la información, se definen los elementos clave para la gestión de riesgo de tecnología de la información como un marco de trabajo definido. A continuación, una breve reseña:

Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización. Otros de los riesgos a los que una organización se enfrenta pueden ser riesgos estratégicos, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos y riesgos de cumplimiento. En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo, por ejemplo, el sector financiero en el marco de Basilea II. Sin embargo, incluso el riesgo estratégico de TI puede tener un componente financiero, especialmente en aquellas organizaciones en las que es el

elemento clave de nuevas iniciativas empresariales. Lo mismo se aplica para el riesgo de crédito, donde una política pobre en cuanto a seguridad de la información se refiere, puede conducir a menores calificaciones de crédito. Por esta razón, es mejor no describir los riesgos de TI con una dependencia jerárquica en una de las categorías de riesgo. (ISACA 2009:11).

El marco de trabajo de Riesgos de la tecnología de la información es el riesgo comercial, es decir, el riesgo de los negocios asociados con el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI dentro de una organización. Se compone de eventos relacionados con IT que podrían afectar a la organización. Esto incluye tanto la frecuencia y la magnitud incierta, la creación de problemas en el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades. Los riesgos pueden clasificarse de varias formas: (ISACA 2009:11).

- El valor de los riesgos de TI permitidos – Asociado con las oportunidades no aprovechadas para mejorar la eficiencia o efectividad de los procesos de negocio, o la capacidad de soportar nuevas iniciativas, a través del uso de la tecnología.

- Programas de TI y riesgos en las entregas de proyectos – Asociada a la contribución de IT sobre nuevas soluciones de negocio, generalmente en forma de proyectos y programas.

- Operaciones de TI y riesgos en las entregas de servicios – Asociadas con todos los aspectos relacionados con los servicios y sistemas de TI, los cuales puede producir pérdidas o reducción del valor a la organización.

Los riesgos relacionados de TI existen, independientemente de si son descubiertos o reconocidos por una organización. En este contexto es importante identificar y gestionar potencialmente los asuntos importantes de riesgo de TI, a

diferencia del resto de riesgos, ya que éste puede no ser rentable. ISACA (2009:11)

El marco de trabajo RISK IT tiene como propósito la correcta gestión de los riesgos a los que está expuesta la organización es esencial para la correcta administración de cualquier organización. Casi todas las decisiones de negocio requieren que alta dirección o los gerentes sopesen los riesgos y los beneficios. El uso común y general de las TI puede proporcionar importantes beneficios a una organización, pero también implica riesgos. Debido a su importancia para las organizaciones, los riesgos relacionados con TI deberían ser tratados como los demás riesgos claves organizacionales, tales como el riesgo del mercado, el riesgo de crédito y otros riesgos operativos. Dichos riesgos los podemos ubicar por debajo de la categoría más crítica de los riesgos en una organización: el hecho de no lograr los objetivos estratégicos del negocio. Si bien estos riesgos han sido incorporados a las organizaciones en los procesos de toma de decisión, muchos ejecutivos tienden a relegar los riesgos a los especialistas técnicos. El marco de trabajo de Riesgos de la tecnología de la información explica los riesgos y permite a los usuarios: (ISACA 2009:11).

- Integrar la gestión de los riesgos en la gestión de los recursos empresariales de la organización, permitirá que se tomen decisiones conscientes sobre el retorno de los riesgos.

- Tomar decisiones con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo y la tolerancia al riesgo de la organización.

- Entender cómo responder a los riesgos.

En resumen, este marco permite a la organización adoptar las decisiones de riesgo apropiadas.

La práctica ha demostrado que la función de TI y los riesgos de TI a menudo no son bien comprendidos por las principales partes interesadas de una organización, entre ellos los miembros de la junta y la dirección ejecutiva. Sin embargo, estas son las personas que dependen de TI para alcanzar los objetivos estratégicos y operativos de la organización y, en consecuencia, deberían ser los 0responsables de la gestión de los riesgos. Sin una clara comprensión de la función y de los riesgos asociados a TI, los ejecutivos de alto rango no tienen un marco de referencia para priorizar y administrar los riesgos de TI. Los riesgos de TI no son puramente una cuestión técnica. A pesar de que se necesita de expertos en la materia para entender y gestionar los aspectos de los riesgos de TI, el conocimiento sobre la gestión del negocio es lo más importante. Los gerentes del negocio han de determinar lo que se debe hacer para apoyar su negocio y establecer los objetivos de TI. Por consiguiente, son responsables de la gestión de los riesgos asociados. (ISACA 2009:12).

En el marco de trabajo de Riesgos de la tecnología de la información, la gestión del negocio incluye los roles o cargos corporativos, líderes del negocio y funciones de apoyo (director financiero, jefe de información, recursos humanos, etc.). Proporciona de principio a fin, visión global de todos los riesgos relacionados con el uso de las TI y un tratamiento igualmente minucioso de la gestión del riesgo, desde el tono y la cultura hasta las cuestiones operativas. En resumen, el marco permitirá a las organizaciones entender y gestionar todos los tipos importantes de riesgos de TI. El Marco provee de: (ISACA 2009:12).

- Un marco de proceso de punta a punta para gestión de riesgos de TI correcta.

- Orientación para los profesionales, incluyendo herramientas y técnicas para entender y gestionar los riesgos concretos para las operaciones de negocio. Esto incluye una lista genérica de campo común, los panoramas

relacionados con la TI potencialmente adversos del riesgo que podrían afectar la realización de los objetivos de negocio.

Tabla 1 - Dirección de audiencia del marco de trabajo de riesgos de TI

Papel	Beneficios de/ Razones para usar el marco de riesgos de TI
Junta y Dirección Ejecutiva	Mejor comprensión de sus responsabilidades y funciones con respecto a la gestión de riesgos de TI.
Gestores de Riesgos	Asistencia con la gestión de los riesgos de TI, de acuerdo con la organización generalmente aceptados por los principios de la gestión de riesgos.
Administrador de los riesgos Operacionales	Marco de su vinculación con los riesgos de TI, la identificación de las pérdidas operativas o el desarrollo de los principales indicadores de riesgo.
Dirección de TI	Mejor comprensión de cómo identificar y gestionar los riesgos y la forma de comunicar los riesgos a la toma de decisiones de negocios
Directores de servicios de TI	Mejora de su punto de vista sobre los riesgos relacionados con TI, los cuales deberían encajar en el conjunto global del marco de trabajo de la gestión de riesgos de IT.
Administrador de la continuidad de negocio	La alineación con la organización de gestión de riesgos (desde la evaluación de riesgo es un aspecto clave de su responsabilidad)
Administrador de seguridad de TI	Posicionamiento de los riesgos de seguridad, entre otras categorías de riesgo de IT
CFOs	Obtener una mejor visión de los riesgos relacionados con TI y sus implicaciones financieras
Oficiales del gobierno organizacional	Asistencia con su examen y la supervisión de las responsabilidades de gobierno y otras funciones de gobierno de TI.
Directores ejecutivos	La comprensión y la gestión de los riesgos es uno de los muchos riesgos de negocios, todos los cuales deben ajustarse.
Los auditores de TI	Mejor análisis de riesgo en apoyo de los planes de auditoría e informes

Papel	Beneficios de/ Razones para usar el marco de riesgos de TI
Reguladores	Apoyo de su evaluación de las organizaciones reguladas —enfoque de gestión de riesgos de TI
Auditores externos	Orientación adicional sobre las tecnologías relacionadas con los niveles de riesgo cuando se crea una opinión sobre la calidad del control interno
Aseguradores	Apoyo en el establecimiento de cobertura de seguro adecuada de TI y la búsqueda de un acuerdo sobre los niveles de riesgo
Las agencias de calificación	En colaboración con aseguradores; una referencia para evaluar objetivamente y la tarifa como una organización se ocupa de los riesgos

Fuente: ISACA (2009:12).

Los beneficios y resultados que ofrece el marco de trabajo de riesgos de la tecnología de la información, son: (ISACA 2009:12)

- Una visión precisa del presente y del futuro próximo sobre los riesgos relacionados con TI en toda la organización y el éxito con el que la organización se ocupa de dichos riesgos.

- Orientación de principio a fin sobre la forma de gestionar los riesgos relacionados con TI, más allá de medidas puramente técnicas de control y de seguridad.

- Comprensión de cómo capitalizar una inversión realizada en un sistema de control interno de TI ya existente para gestionar los riesgos relacionados con TI.

- En cuanto a la evaluación y gestión de los riesgos de TI, la integración con el riesgo global y el cumplimiento de las estructuras dentro de la organización.

- Un marco/lengua común para ayudar a gestionar la relación entre los ejecutivos encargados de adoptar decisiones (o junta de los altos directivos), el director de información y la organización de gestión del riesgo, o entre los auditores y la dirección.

- Promoción de la responsabilidad del riesgo y su aceptación en toda la organización.

- Un perfil de riesgo completo para mejor entender el riesgo y aprovechar mejor los recursos de la organización.

2.4 Marco de trabajo RISK IT para la gestión de riesgo de tecnología de la información

Se consideran para la investigación las siguientes herramientas definidas en el marco de trabajo el marco de trabajo de Riesgos de la tecnología de la información: (ISACA 2009:11).

2.4.1 Roles y responsabilidades

El marco de trabajo de riesgo de TI define el modelo RACI como la base para la rendición de cuentas. RACI proviene del inglés y hace referencia a las responsabilidades más frecuentemente incluidas en la matriz: Responsible, accountable, consulted, e informed. El acrónimo RACI corresponde a:

R = Responsable

A = Rendidor de cuentas

C = Consultado

I = Informado

La responsabilidad corresponde a aquellos que deben velar por que las actividades se han completado con éxito. La rendición de cuentas se aplica a quienes poseen los recursos necesarios y tener la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad específica dentro de los procesos de TI de riesgo. La siguiente tabla es un resumen de los cuadros detallados en el modelo de proceso. Las funciones descritas en la tabla se aplican de manera diferente en cada organización. ISACA (2009:39).

Para esta investigación la matriz RACI del modelo de recolección de datos se definió así:

Tabla 2 - Matriz RACI para modelo de recolección de datos

Actividades Especiales	Alta Gerencia	Gerente General	Gerente de Riesgos	Gerente de TI	Gerente Financiero	Comité de Riesgo	Gestores de Negocios	Dueño de proceso	Controladore de Riesgo	Recursos Humanos	Cumplimiento y Auditoría
Establecer y mantener un modelo para la recolección de datos	I	I	A/R	C	C	C	C	C	C		C
Recopilar datos sobre el entorno externo		I	A/R	C	I	I	C	I	I	I	C
Escoger caso puntual, incidentes, problemas y pérdida de datos		I	A	R	C	I		C	C		I
Identificar los riesgos de TI			A	R	I	I	C	C	R	C	C

Fuente: ISACA (2009:39).

2.4.2 Estándar de seguridad de la información

El sistema de gestión de seguridad de la información (SGSI) el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito

de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

De acuerdo con ISO 27001, la seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

La clasificación de la información, según ISO 27001 (Information Classification Policy), es la siguiente:

- Pública: aquella que, en caso de caer en dominio público, no tiene impacto para la organización como campañas de marketing de temporadas anteriores, inversiones de la empresa, estructura organizacional de la empresa, etc.

- Uso de Negocio: se considera de bajo impacto para la organización en caso llegue a ser de dominio público. Este tipo de información tiene por objeto ser compartida solamente con los empleados de la empresa a cualquier nivel y

se comparte solo quien necesita tenerla. Por ejemplo, planes estratégicos de años anteriores, planificación de proyectos ya efectuados, organigramas de la empresa, políticas de la compañía, etc.

- Confidencial: aquella información que no es disponible a todos los colaboradores de la empresa sino solo aquellos con jerarquía suficiente o involucrados en la iniciativa o proceso de la cual es objeto la información, por ejemplo, planes de promoción interna de personal y escalafones salariales, bonos por desempeño, balances generales, estados financieros proyectados y auditados, multas por evasión de impuestos, registros de clientes, etc. En caso esta información llegue a dominio público, la empresa sufriría serias complicaciones que pueden llegar a restar valor y generar pérdidas financieras por pérdida de participación de mercado por mala reputación, sanciones, demandas, procesos judiciales, etc.

- Estrictamente confidencial: la cual se refiere a información que en teoría solo la alta gerencia de la empresa y algunos otros colaboradores clave debe tener acceso. La publicación de esta información en el dominio público puede llegar a amenazar seriamente la existencia y continuidad de la misma empresa. Ejemplos de este tipo de información pueden ser planes estratégicos, planes de marketing y ventas, información sensible o financiera de clientes, información sobre procesos legales por los que esté pasando la empresa y que resten imagen o credibilidad a la misma, información de proyectos clave o proyectos no exitosos, inversiones en bolsa de valores, información de accionistas, proyectos clave en proceso, entre otros.

2.4.3 Modelo de recolección de datos

Para el modelo de recolección de datos de riesgos de tecnología de la información, se deben identificar los datos pertinentes para hacer viable la

identificación de riesgos de TI relacionados, el análisis y presentación de informes. (ISACA 2009:66).

2.4.3.1 Establecer y mantener un modelo para la recolección de datos

Se debe establecer y mantener un modelo para la recolección, clasificación y análisis de datos de TI de riesgo para acomodar múltiples tipos de eventos (el evento de la amenaza, el evento de la vulnerabilidad, el evento de pérdida) y varias categorías de riesgos de TI para posterior análisis. Estos datos incluyen filtros y puntos de vista para ayudar a determinar los factores de riesgo específicos de cómo llega a afectar el riesgo (p. e., la frecuencia, magnitud, impacto en el negocio). El modelo debe apoyar la medición y evaluación de los atributos de riesgo (por ejemplo, la disponibilidad) a través de los dominios y los riesgos de TI proporcionar datos útiles para el establecimiento de incentivos para una cultura de conciencia de riesgo. (ISACA 2009:66). Los aspectos más relevantes del modelo de recolección que presenta el marco de trabajo de gestión de riesgos de TI son:

2.4.3.2 Recopilar datos sobre el entorno operativo

El modelo de recopilación de datos debe dar registro de datos sobre el entorno operativo de la empresa que podría desempeñar un papel importante en la gestión de las TI. Consultar las fuentes dentro de la empresa, el departamento legal, el de auditoría, el de cumplimiento y la Oficina del Director de TI. Cubrir las principales fuentes de ingresos, los sistemas externos, la responsabilidad del producto, el panorama normativo, la competencia en la industria, las nuevas tendencias en la alineación de los competidores con puntos de referencia fundamentales, la madurez relativa de los principales negocios y capacidades de TI y los problemas geopolíticos. Encuesta y organización de los datos históricos, los riesgos de TI y la experiencia de la pérdida de colegas de la industria a través de la industria basada en los registros de eventos, bases de datos y los acuerdos de la industria para la divulgación de eventos comunes (por ejemplo, la banca debe establecer acuerdos

sectoriales en materia de divulgación de los acontecimientos de fraude generalizado). (ISACA 2009:66).

2.4.3.3 Recopilar datos sobre eventos de riesgo

El modelo de recogida de datos debe dar registro de datos sobre eventos de riesgo que han provocado o provocarían impactos en IT / beneficio de habilitación de valor, los programas y la ejecución de proyectos y / u operaciones de TI y prestación de servicios. Captura de datos relevantes de las cuestiones relacionadas, incidentes, problemas e investigaciones. (ISACA 2009:67).

2.4.3.4 Identificar factores de riesgo

Para las empresas pertinentes para eventos similares, organizar los datos recogidos y poner de relieve los factores contribuyentes. Determinar qué condiciones específicas existían o no existían cuando se registraron los eventos de riesgo y cómo las condiciones han afectado la frecuencia de eventos y la magnitud de la pérdida. Determinar los factores comunes que contribuyen a través de varios eventos. Realizar eventos periódicos y análisis de los factores de riesgo para identificar cuestiones nuevas o incipientes de riesgo y de obtener una comprensión de los factores de riesgo asociados internos y externos. (ISACA 2009:67).

2.4.4 Análisis de riesgos

El marco de trabajo de gestión de riesgos de TI establece que se debe desarrollar información útil para apoyar las decisiones de riesgo que tengan en cuenta la importancia de factores de riesgo de negocios. (ISACA 2009:70).

2.4.4.1 Alcance del análisis de riesgos

Para decidir sobre la amplitud y la profundidad de las expectativas de los esfuerzos de análisis de riesgos se debe considerar la posibilidad de una amplia gama de opciones adicionales, que incluyen: (ISACA 2009:70).

- Requisito de la toma de decisiones estratégicas (por ejemplo, nuevos productos y servicios, nuevo entorno operativo, la externalización, nuevos requerimientos normativos).

- Empresas cuyos resultados de la evaluación de riesgos den zonas de riesgo residual fuera de los umbrales de tolerancia de gestión necesitan un examen más detenido de las operaciones en curso (por ejemplo, la línea de negocio, producto, servicios y procesos – de forma individual o en combinación).

- Mapa de los factores de riesgo pertinentes y la criticidad de los activos de empresas consideradas en el estudio / recursos y factores desencadenantes.

- Objetivo para el valor óptimo del análisis de riesgos.

- Esfuerzos para favorecer el alcance sobre la base de los procesos productivos y productos de la empresa (por ejemplo, la generación de ingresos, atención al cliente, calidad) sobre las estructuras internas que no estén directamente relacionados con los resultados de negocio (por ejemplo, los tipos de hardware, lugares, organizaciones funcionales).

- Establecer el ámbito de aplicación de análisis de riesgos después de un examen de la criticidad de negocios, el costo de la medición contra el valor esperado de la información y reducción de la incertidumbre, y todos los requisitos reglamentarios generales.

2.4.4.2 Estimación de riesgos de TI

A través del alcance del análisis de riesgos de TI, la estimación de la frecuencia probable y la magnitud probable de la pérdida o ganancia asociada con los riesgos de TI deben aplicarse como escenarios de la influencia de los factores de riesgo. La estimación de la cantidad máxima de los daños que pudiera sufrir (por ejemplo, una pérdida del peor caso, cuando convergen los factores de riesgo específicos) o la oportunidad que se podrían obtener. Considerar la posibilidad de escenarios compuestos de cascada y/o tipos de amenaza coincidente (por ejemplo, una amenaza externa más una interna de accidente). Basado en los escenarios más importantes, desarrollar las expectativas de los controles específicos, capacidad de detección y medidas de respuesta. Evaluar los controles operativos conocidos y sus probables efectos sobre la frecuencia y la magnitud probable y los factores de riesgo aplicables. Estimación de los niveles de riesgo residual de la exposición y comparar con la tolerancia de riesgo aceptable para identificar los riesgos que pueden requerir una respuesta de riesgo. (ISACA 2009:71).

2.4.4.3 Identificación de opciones de respuesta de riesgo

Se debe examinar la gama de opciones de respuesta de riesgo, tal como aceptar, explotar, mitigar, transferir o evitar. Justificación de cada uno. Especificar los requerimientos de alto nivel para los proyectos o programas que, basados en la tolerancia de riesgo, mitiguen el riesgo a niveles aceptables o reducir los controles existentes, identificar los costos, beneficios y la responsabilidad de la ejecución del proyecto. Desarrollar los requisitos y las expectativas de los controles de materiales en los puntos más adecuados o cuando se espera que se va a desarrollar para dar visibilidad significativa. (ISACA 2009:71).

2.4.4.4 Realizar una revisión por pares de los resultados de análisis de riesgos de TI

Identificar necesidades de recursos para la gestión de riesgos en el negocio y el nivel de TI y en el contexto de la competencia las cuestiones relativas a los riesgos de negocios, las limitaciones de recursos y objetivos. Asignar los fondos necesarios para llenar las lagunas y la posición de la empresa para aprovechar las oportunidades. Establecer el riesgo/recompensa de comercio externo en relación con los objetivos de la organización (por ejemplo, asignar más o menos recursos sobre la base de la criticidad de los datos dentro de un enfoque escalonado para la seguridad de la información). (ISACA 2009:72).

2.4.5 Administración del riesgo de TI

Para el desarrollo de este tema se incluyen: (ISACA 2009:17).

- El apetito del riesgo y la tolerancia al riesgo
- Responsabilidades y rendición de cuentas sobre la gestión riesgos de TI
- Sensibilización y comunicación
- Cultura del riesgo

2.4.5.1 Apetito de riesgo y tolerancia

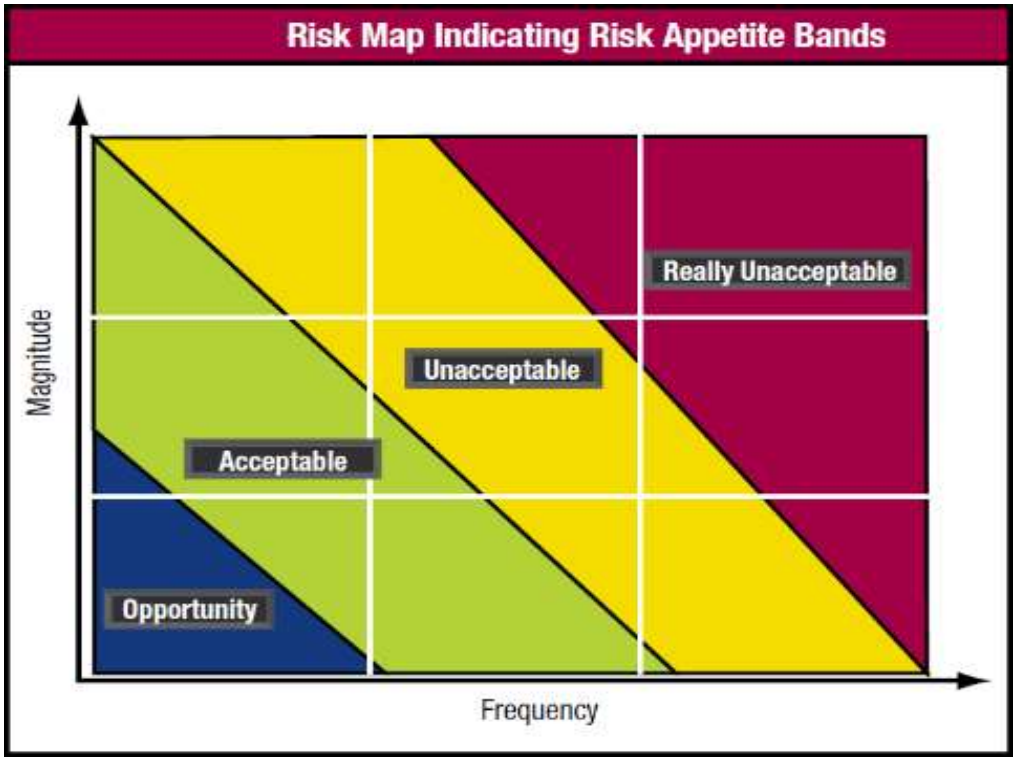
El apetito de riesgo es la cantidad de riesgo que una entidad está dispuesta a aceptar cuando se trata de alcanzar sus objetivos. Al examinar los niveles de apetito para la organización, surgen dos grandes factores importantes:

- La Capacidad Objetiva de la organización para absorber pérdida, por ejemplo., pérdida financiera, daño de reputación

- La cultura o la predisposición a asumir riesgos-prudentes o agresivos. ¿Cuál es la cantidad de pérdida que la organización quiere aceptar llevar a cabo?

El apetito de riesgo se define en la práctica en términos de combinaciones de la frecuencia y la magnitud de un riesgo. El apetito de riesgo va a ser diferente entre las organizaciones ya que no existe una norma absoluta o una norma de lo que constituye un riesgo aceptable e inaceptable. El apetito por el riesgo se define mediante los mapas de riesgo. Diferentes grupos de riesgo se definen indicado nivel de importancia por bandas de colores en el mapa de riesgo se muestra en la Ilustración" (ISACA 2009:17).

Ilustración 1 - Mapa de Riesgo que Indica las bandas de apetito de Riesgo



Fuente: ISACA (2009:17).

Se definen cuatro bandas de importancia:

- Rojo - indica que realmente es un riesgo inaceptable. La organización estima que este nivel de riesgo es mucho más allá de su apetito de riesgo normal. Cualquier riesgo que se encuentren en esta banda podría desencadenar una respuesta inmediata de riesgos.

- Amarillo: indica riesgo elevado, es decir, también por encima de apetito de riesgo aceptable. La organización podría aceptarlo, como cuestión de política. Requieren mitigación u respuesta adecuada a definir dentro de los límites de tiempo determinado.

- Verde: indica un nivel aceptable normal de riesgo, normalmente con ninguna acción especial requerida, excepto el mantenimiento de los controles actuales o de otras respuestas.

- Azul -indicio de un riesgo muy bajo, donde el ahorro del costo de oportunidades se puede encontrar al disminuir el grado de control o donde las oportunidades para asumir más riesgos pueden surgir.

La tolerancia al riesgo es la desviación tolerable desde el nivel establecido por la definición del apetito de riesgo, por ejemplo, las normas o proyectos que deben realizarse dentro de los presupuestos y el tiempo, pero sobre costes del 10 por ciento del presupuesto o el 20 por ciento del tiempo son tolerados. (ISACA 2009:17).

Con respecto a la sensibilización y comunicación, la concienciación de los riesgos es de reconocer que el riesgo es una parte integral de la organización. Esto no implica que todos los riesgos que deben ser evitadas o eliminadas, sino que se entienden y conocen los riesgos de TI, problemas de riesgo sean identificables, y la organización reconoce y utiliza los medios de manejar los riesgos de TI. (ISACA 2009:18).

La gestión de riesgos consiste en ayudar a las organizaciones a asumir mayores riesgos en la búsqueda de la rentabilidad, por lo que una cultura de riesgos asumidos ofrece un entorno en el que los componentes de riesgo se discuten abiertamente, y los niveles de riesgo aceptables se entienden y se mantienen. La cultura de riesgos aceptables comienza en la parte superior, con la junta y los ejecutivos de negocios que establece la dirección, comunicando el riesgo de toma de decisiones aceptables y premiando la cultura de aprendizaje en la gestión eficaz del riesgo. El conocimiento del riesgo también implica que todos los niveles dentro de una organización son conscientes de cómo y por qué para responder a los eventos adversos de TI. (ISACA 2009:19).

2.4.6 Reacción a los acontecimientos

La reacción a los eventos de riesgo se define como: Asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con la TI se activan en forma oportuna y eficaz. ISACA (2009:91).

El marco de trabajo de riesgos de TI define aspectos relevantes para la definición de planes de mitigación de riesgo. Entre los aspectos de interés se plantean los siguientes:

2.4.6.1 Mantener los planes de respuesta a incidentes

La organización debe prepararse para la materialización de amenazas a través de planes que se establecen en un documento de medidas específicas a tomar cuando se produce un evento de riesgo operacional, de desarrollo y / o impacto en el negocio estratégico (es decir, incidente relacionado), o ya ha causado un impacto en el negocio. Se debe mantener una comunicación abierta sobre la aceptación de riesgos, actividades de gestión de riesgos y técnicas del análisis y los resultados disponibles para ayudar con la preparación del plan. En el desarrollo de planes de acción, considere cuánto tiempo la empresa está expuesta

y por cuánto tiempo tardaría en recuperarse. Con base en los efectos conocidos o potenciales, definir las vías de escalada en toda la empresa, desde la gestión en línea a los comités ejecutivos. Finalmente, Comprar que los planes de respuesta a incidentes de procesos altamente críticos son los adecuados. ISACA (2009:91)

2.4.6.2 Supervisión de riesgos de TI

Supervisar el ambiente. Cuando un límite de control ha sido violado, o bien aumentan con el paso siguiente o confirmar que la medida está de vuelta dentro de límites previamente establecidos. Se debe categorizar los incidentes (por ejemplo, pérdida de negocio, violación de la política, el fracaso del sistema, el fraude, la demanda), y comparar las exposiciones reales contra los umbrales aceptables. Finalmente comunicar los impactos comerciales a los tomadores de decisiones. Continuar con la unidad de acción y los resultados deseados. Garantizar la política se sigue y que hay una clara responsabilidad por las acciones de seguimiento. ISACA (2009:91).

2.4.6.3 Iniciar planes de respuesta a incidentes

Se debe adoptar medidas para minimizar el impacto de un incidente en el progreso. Identifique la categoría de los hechos y seguir los pasos en el plan de respuesta. Informar a todas las partes interesadas y afectadas que un incidente que está ocurriendo. Identificar la cantidad de tiempo necesario para llevar a cabo el plan y hacer los ajustes que sean necesarios, para la situación a la mano, asegurando tomar la acción correcta. ISACA (2009:91).

2.4.6.4 Comunicar las lecciones aprendidas de eventos de riesgo

Examinar los últimos acontecimientos adversos y pérdidas. Determinar si hubo una falla derivados de la falta de conciencia, la capacidad o la motivación. De Investigación de la causa raíz de los acontecimientos históricos similares adversos o pérdidas y la eficacia relativa de las medidas adoptadas entonces y ahora.

Determinar el alcance de los problemas subyacentes (por ejemplo, un problema sistémico grave contra un caso aislado que pueda ser manejada a través de la formación del personal o una mayor documentación de los procedimientos). Para las operaciones de TI y los incidentes relacionados con la prestación de servicios de TI ofertas de servicios y niveles de servicio (por ejemplo, defectos, reparación), la integración con la oficina de servicio de TI y el proceso de respuesta a incidentes y el proceso de gestión de problemas de TI para identificar y corregir la causa subyacente. La identidad de la causa raíz del problema beneficio / valor y la habilitación de programas y proyectos de incidentes de entrega mediante la comunicación abierta a través de negocios y funciones de TI. ISACA (2009:92).

Solicitar análisis de riesgo adicionales como sea necesario. Comunicar causa, los requisitos adicionales de respuesta de riesgos y mejora de los procesos de riesgo para los procesos de gobierno y toma de decisiones adecuadas. (ISACA (2009:92).

2.4.7 Gestión de riesgo empresarial

Según Kogan (2017), existen tres componentes requeridas para una definición holística del proceso de gestión de riesgo empresarial:

1. La descripción de los procesos respecto de la gestión de riesgo
2. La identificación de las salidas de esos procesos
3. El impacto o beneficio que generan esas salidas de proceso”

La gestión de riesgo empresarial, para ser holística, considera la identificación y evaluación de riesgos significativos, asignación de rendición de cuentas, implementación y monitoreo de las acciones para gestionar los riesgos dentro del apetito de riesgo de las organizaciones. El resultado de gestionar riesgos es la provisión de información para que los gestores de negocio mejoren sus decisiones

de negocio, reduciendo la incerteza y generando seguridad razonable respecto de la consecución de los objetivos de la organización. (Kogan 2017:4).

El impacto de la gestión de riesgo empresarial es mejorar la eficiencia y la entrega de servicios, mejorando la distribución de recursos de capital a las mejoras de las operaciones de negocio, crear valor para los inversionistas y/o propietarios, así como mejorar la manera en la que se reportan los riesgos a los interesados. (Kogan 2017:4).

2.5 Administración financiera

De acuerdo con Van Horne y Wachowicz (2010), el director financiero (CFO, por las siglas de chief financial officer) desempeña un papel dinámico en el desarrollo de una compañía moderna. Ahora, los factores externos tienen un efecto creciente, una mayor competencia corporativa, el cambio tecnológico, la volatilidad en la inflación y las tasas de interés, la incertidumbre económica mundial, las tasas de cambio fluctuantes, los cambios en las leyes fiscales, los aspectos ambientales y las preocupaciones éticas en algunos tratos financieros son asuntos cotidianos. Como resultado, las finanzas deben desempeñar un papel estratégico importante dentro de la corporación. El director financiero emerge como un miembro del equipo en el esfuerzo global de una compañía por crear valor.

Ante esta situación toma relevancia la administración financiera, que se ocupa de la adquisición, el financiamiento y la administración de bienes con alguna meta global en mente. La función de decisión de la administración financiera puede desglosarse en tres áreas importantes: decisiones de inversión, financiamiento y administración de bienes. La decisión de inversión es la más importante de las tres decisiones primordiales de la compañía en cuanto a la creación de valor. Comienza con una determinación de la cantidad total de bienes necesarios para la compañía. La segunda decisión importante de la compañía es la decisión financiera, la mezcla de financiamiento, la fuente de financiamiento, por lo que

debe entenderse la mecánica para obtener un préstamo a corto plazo, hacer un acuerdo de arrendamiento a largo plazo o negociar una venta de bonos o acciones. La tercera decisión importante de la compañía es la administración de bienes que se adquieren, aunque una gran parte de la responsabilidad de la administración de activos fijos recae en los gerentes operativos que emplean esos bienes. (Van Horne y Wachowicz 2010).

2.5.1 Herramientas de análisis financiero

Para tomar decisiones racionales y cumplir con los objetivos de la empresa, se deben tener herramientas analíticas. La empresa en sí y los proveedores de capital externos (acreedores e inversionistas) emprenden el análisis de los estados financieros. El tipo de análisis varía de acuerdo con los intereses específicos de quien lo realiza. Los acreedores (proveedores de dinero para bienes y servicios) están interesados principalmente en la liquidez de la empresa. Sus demandas son a corto plazo, y la habilidad de pagar estas demandas con rapidez se juzga mejor mediante el análisis de liquidez de la empresa. Las demandas de los accionistas, por otro lado, son a largo plazo. De acuerdo con esto, los accionistas están más interesados en la capacidad de la empresa para manejar flujos de efectivo y pagar el servicio de la deuda en un periodo largo. Pueden evaluar esta capacidad analizando la estructura del capital, las fuentes más importantes y los usos de los fondos, la rentabilidad de la empresa en el tiempo y las proyecciones de rentabilidad futura. (Van Horne y Wachowicz 2010).

Internamente, la administración también emplea el análisis financiero para fines de control interno y para ofrecer a los proveedores de capital lo mejor en cuanto a condiciones financieras y desempeño de la empresa. Desde el punto de vista de control interno, la administración necesita realizar un análisis financiero para planear y controlar con efectividad. Para planear el futuro, el gerente financiero debe evaluar la posición financiera actual de la compañía y las oportunidades relacionadas con esta posición. En cuanto a control interno, el gerente financiero

está interesado en particular en el rendimiento sobre la inversión en los diferentes bienes de la compañía y en la eficiencia de la administración de los bienes. Por último, para negociar con efectividad los fondos externos, necesita estar en concordancia con todos los aspectos del análisis financiero que los proveedores de capital externos usan para evaluar a la empresa. Así, vemos que el tipo de análisis financiero realizado varía según los intereses específicos del analista. (Van Horne y Wachowicz 2010).

2.5.2 Estados financieros

El análisis financiero implica el uso de varios estados financieros. Estos estados hacen varias cosas. Primero, el balance general resume los bienes, pasivos y el capital de los dueños de un negocio en un momento, generalmente al final del año o de un trimestre. Luego, el estado de pérdidas y ganancias resume los ingresos y gastos de la compañía durante un periodo determinado, por lo general un año o un trimestre. Aunque el balance general representa una fotografía de la posición financiera en ese momento, el estado de pérdidas y ganancias describe un resumen de la rentabilidad en el tiempo. De estos dos estados (en algunos casos, con un poco de información adicional), se pueden obtener ciertos estados derivados, como un estado de utilidades retenidas, un estado de fuentes y uso de fondos, y un estado de flujos de efectivo.

2.5.3 Estado de resultados o de pérdidas y ganancias

El estado de ingresos (de utilidades, o de pérdidas y ganancias) muestra los ingresos, los gastos y las ganancias netas. El costo de los bienes vendidos representa el costo de fabricación real de los productos que se vendieron durante el periodo. Incluye el costo de las materias primas, la mano de obra asociada con la producción y los gastos generales relacionados con los productos vendidos. Los gastos de ventas, generales y administrativos al igual que los gastos en intereses

se muestran separados de los costos de vender bienes porque se ven como gastos del periodo y no como costos de producción.

Para una compañía de manufactura, el gasto por depreciación generalmente se considera un componente del costo de los bienes producidos y, por lo tanto, se convierte en parte del costo de los bienes vendidos. Para una empresa comercializadora (al mayoreo o al menudeo), la depreciación casi siempre se pone separada, como el gasto de otro periodo (igual que el gasto en intereses) abajo de la cifra de ganancia bruta. La depreciación está basada en datos históricos de costos, que en un periodo de inflación puede no corresponder a los costos económicos.

Tabla 3 - Estado de resultados (1)

	Año 20X2
	$
Ventas netas (2)	3,992
Costo de bienes vendidos (3)	2,680
Ganancia bruta	**1,312**
Gastos de ventas, generales y administrativos (4)	912
Utilidad antes de intereses e impuestos (5)	400
Gastos de interés (6)	85
Utilidad antes de impuestos (7)	**315**
Impuesto sobre la renta (federales y estatales)	114
Utilidad después de impuestos (8)	**201**
Dividendos en efectivo	143
Incremento de utilidades retenidas	58

Nota: los gastos por depreciación fueron $114.

Fuente: Van Horne y Wachowicz (2010).

Explicaciones:

1. Medidas de rentabilidad en un período

2. Cantidad recibida o por cobrar de los clientes

3. Directamente relacionados con los niveles de operación: salarios, materias primas, suministros y costos generales de manufactura.

4. Comisiones de ventas, publicidad, salarios de funcionarios

5. Ingreso operativo.

6. Costo de fondos en préstamos.

7. Ingreso gravable.

8. Cantidad ganada por los accionistas.

2.5.4 Flujos de fondos (fuentes y usos)

El arreglo del flujo de fondos de una compañía de manera sistemática, permite determinar mejor si las decisiones tomadas dieron como resultado un flujo de fondos razonable o flujos cuestionables que necesitan mayor inspección. Los fondos están en efectivo (o son equivalentes de efectivo). El interés debe centrarse en las transacciones que tienen efecto sobre las cuentas de efectivo, que afectan los flujos de entrada y de salida del efectivo. Pero definir los fondos como efectivo es limitante. Un análisis de flujo de fondos en el que éstos se definen estrictamente como efectivo no toma en cuenta las transacciones que no afectan directamente el “efectivo”, y estas transacciones pueden ser cruciales para una evaluación completa del negocio. Compras importantes de fin de periodo y ventas a crédito, la adquisición de propiedad a cambio de acciones o bonos, y el intercambio de una propiedad por otra son sólo unos cuantos ejemplos de transacciones que no se reportarían en un estado de flujo de fondos o de efectivo. Ampliar el concepto de fondos para incluir todas las inversiones y reclamaciones (contra esas inversiones) permite considerar todas estas transacciones como fuentes y como usos de los fondos. (Van Horne y Wachowicz 2010).

Se debe resaltar que el estado de flujos de fondos describe los cambios netos y no brutos entre dos balances generales comparables en fechas distintas. Por ejemplo, puede pensarse que los cambios brutos incluyen todos los cambios ocurridos entre dos fechas de balance, y no la suma de estos cambios; es decir, el cambio neto según se definió. Aunque en general dan un panorama amplio de los fondos, los estados de fondos resultantes con frecuencia se centran en el cambio en la posición de efectivo de la empresa con el paso del tiempo o su cambio en el capital de trabajo neto (activos corrientes menos pasivos corrientes). El análisis del flujo de fondos brutos de una empresa en el tiempo es mucho más revelador que el análisis de flujos de fondos netos. (Van Horne y Wachowicz 2010).

Fields (2016), explica que en el pasado, al flujo de caja se le llamaba “fuente y uso de los fondos”, lo cual es una descripción más gráfica de lo que realmente es. Describe resumidamente como las organizaciones generan ingresos (fuentes) para financiar sus diferentes oportunidades y responsabilidad (usos) durante el último año. A continuación se presenta un ejemplo de un flujo de caja.

Tabla 4 - Flujo de caja

Concepto	(Expresado en GTQ)	Año 0
Ingresos		**2,000**
Venta Activos		2,000
Valor de rescate cortafuegos		
Egresos		**- 62,741**
PC Emp 1	Compra Licencias Antivirus	- 1,190
PC Emp 2	Adquisición Cortafuegos	- 12,051
e-mail 1&3	Entrenamientos empleados	**- 7,800**
PC Emp 3 / e-mail 2	Compra Licencias Windows 10	- 11,700
Imp_Fact 1&2 Imp_Admon 1&2	Leasing	- 30,000
Utilidad Neta		**- 60,741**
Impuestos 25%		- 15,185
Flujo de Caja		**- 45,556**

Fuente: Elaboración propia, con base en información de la investigación realizada.

2.5.5 Estados financieros pro forma

Según lo explican Gitman y Zutter (2012), los accionistas, los acreedores y la administración de la compañía prestan mucha atención a los estados financieros pro forma, que son estados de resultados y balances generales proyectados. Todos los métodos para calcular los estados pro forma se basan en la creencia de que las relaciones financieras reflejadas en los estados financieros pasados de la firma no cambiarán en el siguiente periodo. Se requieren dos entradas para elaborar los estados pro forma: 1. los estados financieros del año anterior y 2. el pronóstico de ventas del año siguiente. Del mismo modo que para el presupuesto de caja, la entrada clave para los estados pro forma es el pronóstico de ventas con base en datos externos e internos. Además, se deben hacer varias suposiciones, tales como aumento del precio de venta, para cubrir el aumento esperado en costos.

El método del porcentaje de ventas es un método sencillo para desarrollar un estado de resultados pro forma. Pronostica las ventas y después expresa los diversos rubros del estado de resultados como porcentajes de las ventas proyectadas. Es probable que los porcentajes usados correspondan a los porcentajes de ventas de esos rubros en el año anterior. La técnica que se usa para elaborar el estado de resultados pro forma supone que todos los costos y gastos de la empresa son variables; es decir que para un aumento porcentual determinado en las ventas, se generará el mismo aumento porcentual del costo de los bienes vendidos, los gastos operativos y los gastos por intereses. Como este método supone que todos los costos son variables, puede subestimar el aumento en las utilidades que se presentarán cuando se incrementen las ventas si algunos de los costos de la empresa son fijos. De forma análoga, si las ventas disminuyen, el método del porcentaje de ventas puede sobrestimar las utilidades si algunos de los costos son fijos y no disminuyen cuando los ingresos declinan. Así, un estado de resultados pro forma que se elabora usando el método de porcentaje de ventas generalmente tiende a subestimar las utilidades cuando las ventas aumentan y a sobrestimar las utilidades cuando las ventas disminuyen. (Gitman y Zutter 2012).

Para evitar los problemas anteriores, la mejor forma de ajustar la presencia de costos fijos al elaborar un estado de resultados pro forma es clasificar los costos y gastos históricos de la empresa en componentes fijos y variables. El punto clave a identificar aquí es que los costos fijos hacen más variables las utilidades de una empresa que sus ingresos. Es decir, cuando tanto las utilidades como las ventas se elevan, las utilidades tienden a crecer a un ritmo más rápido, pero cuando las utilidades y las ventas disminuyen, el porcentaje de disminución en las utilidades con frecuencia es mayor que el ritmo de disminución en las ventas. (Gitman y Zutter 2012).

Tabla 5 – Estados de resultados real y proforma

	Real	Proforma
Ingresos por ventas	**100,000**	**135,000**
Menos: Costo de los bienes vendidos	80,000	94,000
Costo fijo	40,000	40,000
Costo variable (0.40 x ventas)	40,000	54,000
Utilidad bruta	**20,000**	**41,000**
Menos: Gastos operativos	10,000	11,750
Gastos fijos	5,000	5,000
Gastos variables (0.05 x ventas)	5,000	6,750
Utilidad operativa	**10,000**	**29,250**
Menos: Gastos por intereses (fijos)	1,000	1,000
Utilidad neta antes de impuestos	**9,000**	**28,250**
Menos: Impuestos (0.15 x utilidad neta antes de impuestos)	1,350	4,238
Utilidad neta después de impuestos	**7,650**	**24,013**

Fuente: Gitman y Zutter (2012).

2.5.6 Caso de negocio

De acuerdo con ISACA (2007: 10), en el proceso de gestión de inversiones, las semillas del éxito o fracaso se siembran en el caso de negocio. Sin embargo, las organizaciones en general no son muy hábiles en el desarrollo y documentación de casos de negocio completos y comparables. El caso de negocio contiene un conjunto de opiniones y suposiciones sobre cómo se puede crear valor. Para garantizar la consecución de los resultados esperados, es necesario que dichas opiniones y suposiciones estén probadas. Unos indicadores cualitativos y cuantitativos permiten la validación del caso de negocio y dan ideas para las decisiones inversoras en el futuro. El uso de guías facilitan la maximización de la calidad de los casos de negocio, poniendo especial énfasis en la definición de indicadores claves, tanto financieros (valor neto actual, tasa interna de rentabilidad y período de recuperación) como no financieros, y en la evaluación y valoración

global del riesgo de pérdidas. El caso de negocio no es un documento puntual y estático, sino una herramienta operativa que hay que actualizar continuamente para reflejar la realidad y para dar soporte al proceso de gestión de cartera.

El caso de negocio (desestimado con demasiada frecuencia como obstáculo burocrático que hay que superar con el mínimo esfuerzo posible) es una de las herramientas más valiosas disponibles para la dirección, para guiarle en la creación de valor de negocio. La experiencia ha demostrado que la calidad del caso de negocio y de los procesos implicados en su creación y uso durante todo el ciclo de vida económico de una inversión, tiene un impacto enorme en la creación de valor. (ISACA 2007:11).

Los casos de negocio tienen que dar respuesta a las cuatro interrogantes, basadas en información relevante enfocada en el negocio sobre los futuros programas: (ISACA 2007:11).

1. ¿Estamos haciendo lo correcto? ¿Qué se propone y para qué resultado de negocio, y cómo contribuyen los proyectos dentro del programa?

2. ¿Lo estamos haciendo correctamente? ¿Cómo se va a hacer, y qué se está haciendo para asegurar su encaje con otras capacidades actuales o futuras?

3. ¿Lo estamos logrando bien? ¿Qué plan tenemos para hacer el trabajo, y qué será necesario en cuanto a recursos y financiación?

4. ¿Estamos obteniendo los beneficios? ¿Cómo se van a entregar los beneficios? ¿Cuál es el valor del programa?

El proceso de desarrollo del caso de negocio debe ser propiedad del promotor del negocio e involucrar a todos los socios claves en el desarrollo y documentación de un conocimiento completo y compartido de los resultados de negocio esperados (resultados tanto intermedios como finales) de una inversión. Debe describir cómo se van a medir los resultados del negocio, así como el alcance de las iniciativas

necesarias para lograr los resultados esperados. Entre estas iniciativas, se debe incluir cualquier cambio necesario en la naturaleza del negocio de la empresa, los procesos de negocio, las habilidades y competencias personales, la tecnología impulsora y la estructura organizacional. En el caso de negocio, se identifica la naturaleza de la contribución de cada iniciativa, como se va a medir dicha contribución, y todas las suposiciones claves. En el caso de negocio, se deben establecer también las métricas o indicadores similares para el monitoreo de la validez de dichas suposiciones. También es necesario identificar y documentar los riesgos principales, tanto para la realización con éxito de las iniciativas individuales como para la consecución de los resultados deseados, junto con las acciones de mitigación. (ISACA 2007:11).

Para la definición de la estructura del caso de negocio se deben tener en cuenta las siguientes relaciones causales: (ISACA 2007:12).

~ Los recursos son necesarios para desarrollar: ~ Un/a tecnología/servicio de TI que dará soporte a: ~ Una capacidad operacional que generará: ~ Una capacidad de negocio que creará: ~ Valor para los socios, que puede ser representado por un rendimiento financiero ajustado por riesgo o por un rendimiento accionarial total.

2.5.7 Pérdida financiera o pérdida de valor

Según Gilbert (2016), la definición de pérdida financiera es la siguiente: “Pérdida financiera o pérdida económica es la destrucción de la oportunidad económica. Sucede cuando una organización reduce su límite de producción, distribución o consumo de bienes. Es, por ejemplo, una amenaza que retira del mercado un producto de una compañía farmacéutica generando pérdida de producción ahora y en el futuro. Debido a lo anterior existe pérdida de oportunidad económica. Desde el punto de vista de la sociedad, el medicamento retirado pierde consumo, generando reducción de ganancias, generando a la vez posible pérdida a los

empleados y dueños de la compañía. Reduce también la disponibilidad del producto y la innovación, reduciendo también el consumo y la salud del público en general.”

Para efectos de la investigación se definen las siguientes categorizaciones de riesgo financiero:

No significativo: No tiene consecuencias relevantes a las finanzas de la empresa.

Bajo: Tiene consecuencias mínimas y plantea recuperación de valor en corto plazo con esfuerzo mínimo por parte de la empresa.

Medio: Tiene consecuencias considerables y plantea recuperación de valor en mediano plazo con esfuerzo medio por parte de la empresa. Puede poner o no en riesgo la salud financiera de la organización.

Alto: Plantea consecuencias financieras severas y con recuperación de valor a largo plazo. Se considera el tipo de riesgo que potencialmente dificultaría alcanzar los resultados reduciendo considerablemente el potencial de generación de rentabilidad.

Crítico: Impacto severo que atenta con la vida misma de la empresa y que tiene como consecuencias la no rentabilidad de los ejercicios operativos. La recuperación de este tipo de impactos es incierta.

3. METODOLOGÍA

La Metodología de investigación explica en detalle de qué y cómo se hizo para resolver el problema de la investigación relacionado con la gestión de riesgo de los activos informáticos en medianas empresas ferreteras de la ciudad de Guatemala.

3.1 Definición del problema

El sector de las medianas empresas ferreteras en la ciudad de Guatemala, realiza un importante aporte a la actividad económica, dedicándose principalmente a la venta de distintos tipos de productos de manufactura extranjera, para proyectos relacionados con la construcción, decoración y remodelación; asimismo ofrecen distintos tipos de herramientas y materiales para actividades de carpintería, construcción, mecánica automotriz, pintura, electricidad, iluminación, cerrajería, plomería, entre otras.

El sector de ferreterías medianas de la ciudad de Guatemala ha intensificado el uso de la tecnología de la información (TI) en la administración y ejecución de procesos de negocio, para el manejo de la cartera de clientes, ingresos y egresos de efectivo, ventas, compras, proveedores, costos y gastos de operación, inventarios, entre otros. Las operaciones se apoyan en sistemas de información y/o por medio del apoyo de otro tipo de componentes tecnológicos a los cuales se les puede llamar también activos informáticos. Estos activos, son componentes que apoyan a la ejecución de procesos de negocio, los cuales deben funcionar en forma continua para no afectar la buena marcha de las empresas.

El uso de la tecnología de la información aumenta la eficiencia de las empresas; sin embargo, implica riesgos operacionales relacionados con los activos informáticos, por falta de adecuación o fallas en los procesos internos, personal, fallas inesperadas en los sistemas, o bien la ocurrencia de eventos externos adversos.

El problema de la presente investigación financiera, se ha enfocado a la realización del diagnóstico de la situación de la administración de los riesgos de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala, en vista de que se ha detectado que carecen de un adecuado sistema para la administración de riesgos de los activos informáticos que permita prevenir o reducir pérdidas financieras por fallas o interrupciones en los procesos.

La propuesta de solución al problema consiste en evaluar la conveniencia de la aplicación del marco de trabajo RISK IT (Riesgo de Tecnología de la Información) como una opción para que las empresas puedan administrar eficientemente los riesgos detectados y aplicar medidas adecuadas de mitigación, para la adecuada seguridad y gestión de los riesgos de activos informáticos, basado en los conceptos de valor y beneficios, y el cumplimiento de los objetivos organizacionales.

3.2 Objetivos

La propuesta de un sistema de gestión de riesgos informáticos en las medianas empresas de Guatemala, con base en el marco de trabajo RISK IT, plantea los siguientes objetivos de investigación.

3.2.1 Objetivo general

Desarrollar un sistema de gestión de riesgo de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala, con base en el marco de trabajo RISK IT (Riesgo de Tecnología de la Información), para integrar la gestión de riesgos a la toma de decisiones, con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo, la tolerancia al riesgo y la respuesta de la organización a los riesgos.

3.2.2 Objetivos específicos

1. Diseñar un modelo para la recolección de datos de los riesgos de los activos informáticos y la tecnología de la información utilizada para los negocios, incluyendo el entorno operativo, eventos de riesgo y factores de riesgo, para la construcción de la matriz de riesgos de activos informáticos, la matriz de procesos de negocio y la ponderación de factores de riesgo.

2. Desarrollar la matriz de evaluación de riesgos de tecnología de la información (TI), con base en el modelo RACI (por sus siglas en inglés, de Responsible, accountable, consulted, e informed) que corresponde a: Responsable, rendidor de cuentas, consultado e informado, como base para la rendición de cuentas de los que deben velar por que las actividades se realicen con éxito.

3. Analizar los resultados de la matriz de evaluación de riesgos de activos informáticos, con base en el análisis de procesos, frecuencia e impacto financiero, para establecer la escala de impacto financiero, en categorías y en unidades monetarias.

4. Crear el mapa de apetito de riesgo de TI, con base en la matriz de evaluación de riesgos, como herramienta visual para determinar el nivel de importancia en cuatro bandas: Rojo, riesgo inaceptable; amarillo, riesgo elevado; verde, nivel aceptable o normal de riesgo; y, azul, riesgo muy bajo.

5. Definir un plan de mitigación de riesgos de activos informáticos con base en el marco de trabajo RISK IT con el fin de priorizar riesgos y analizar el impacto financiero de su ocurrencia tomando en cuenta escenarios optimista y pesimista.

6. Elaborar el estado de resultados pro forma normal, y en escenarios optimista y pesimista, para analizar el impacto de pérdidas en ventas, inventarios, gastos de administración y pérdida total.

7. Definir actividades de mitigación para la respuesta a los riesgos de activos informáticos catalogados en un nivel de riesgo inaceptable, para analizar impacto financiero y la gestión de riesgo post mitigación.

3.3 Hipótesis

El diseño e implementación de un sistema de gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información), en las medianas empresas ferreteras de la ciudad de Guatemala, permite integrar la gestión de riesgos a la toma de decisiones; la construcción de la matriz de riesgo de activos informáticos, la matriz de procesos de negocio y la ponderación de factores de riesgo; la creación del mapa de apetito al riesgo de TI; la definición de un plan de mitigación de riesgos; el análisis del impacto de pérdidas financieras por materialización de riesgos; el análisis de escenarios optimista y pesimista; y, la definición de actividades de mitigación para la respuesta a los riesgos de activos informáticos catalogados en un nivel inaceptable y estrictamente inaceptable.

3.3.1 Especificación de variables

Las variables de la hipótesis son las siguientes:

Variable Independiente

Gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información).

.**Variables dependientes**

Los resultados de la investigación, permitieron:

- La construcción de la matriz de riesgo de activos informáticos, la matriz de procesos de negocio y la ponderación de factores de riesgo.

- La creación del mapa de apetito al riesgo de TI.
- La definición de un plan de mitigación de riesgos.
- El análisis del impacto de pérdidas financieras por materialización de riesgos.
- El análisis de escenarios optimista y pesimista.
- La definición de actividades de mitigación para la respuesta a los riesgos de activos informáticos catalogados en un nivel inaceptable y estrictamente inaceptable.

3.4 Método científico

El presente trabajo de investigación sobre la gestión de riesgo de los activos informáticos en medianas empresas ferreteras de la ciudad de Guatemala, se fundamentó en la utilización del método científico.

Para el efecto, se utilizó un enfoque de investigación cuantitativo, siguiendo los lineamientos expuestos por Hernández et al. (2014), de planteamiento del problema, medición, prueba de hipótesis, generalización de resultados, precisión, réplica y predicción. El enfoque se aplicó empleando procesos cuidadosos, metódicos y empíricos para generar conocimiento, utilizando cinco estrategias relacionadas entre sí:

1. Observación y evaluación del problema.
2. Suposiciones o ideas que resultaron de la observación y evaluación, realizadas.
3. Demostración del grado en que las suposiciones o ideas tienen fundamento.
4. Revisión de las suposiciones o ideas sobre la base de las pruebas o del análisis.

5. Proposición de nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar las suposiciones e ideas o incluso para generar otras.

La investigación partió de una idea que fue delimitándose, se plantearon objetivos y preguntas de investigación, se revisó la literatura y se construyó un marco o una perspectiva teórica. De las preguntas se estableció la hipótesis o respuesta tentativa al problema y se determinó la especificación de variables; se elaboró un plan de investigación para probarla; se midieron las variables; se analizaron las mediciones obtenidas y se extrajeron una serie de conclusiones como resultado de la investigación.

3.5 Técnicas de investigación aplicadas

Dentro de las técnicas utilizadas para este estudio, se especifican como útiles y que generan valor las siguientes:

3.5.1 Técnicas de investigación documental

Las técnicas de investigación documental sirvieron de base para el desarrollo de la perspectiva teórica, a través de la revisión de la literatura disponible y la construcción del marco teórico que contiene la exposición y análisis de las teorías y enfoques teóricos y conceptuales utilizados para fundamentar la investigación.

El desarrollo de la perspectiva teórica siguió el proceso para una investigación cuantitativa, sugerido por Hernández et al. (2014):

- Revisar la literatura.
- Detectar la literatura pertinente.
- Obtener la literatura pertinente.

- Consultar la literatura pertinente.
- Extraer y recopilar la información de interés.
- Construir el marco teórico.

El desarrollo de la perspectiva teórica permitió conocer el estado del conocimiento, con respecto al sector objeto de estudio y la base teórica propuesta de solución al problema de investigación, para orientar el estudio, establecer la necesidad de la investigación, ayudar a la formulación de la hipótesis y proveer de un marco de referencia.

3.5.2 Técnicas de investigación de campo

Las técnicas de investigación de campo, es la parte de la metodología, que permite explicar en detalle qué y cómo se hizo para resolver el problema de investigación. Esencialmente, estas técnicas permitieron la recolección de datos, para un proceso de investigación cuantitativa, para lo cual se siguieron los pasos sugeridos por Hernández et al. (2014):

- Definir la forma idónea de recolectar los datos de acuerdo con el planteamiento del problema y las etapas previas de la investigación.
- Seleccionar o elaborar uno o varios instrumentos o métodos para recolectar los datos requeridos.
- Aplicar los instrumentos o métodos.
- Obtener los datos.
- Codificar los datos.
- Archivar los datos y prepararlos para su análisis.

El resumen del procedimiento usado en el desarrollo de la investigación, se expresa de la siguiente manera:

- Se recolectaron datos de procesos de negocio y activos informáticos con el fin de descubrir evidencias de riesgos con base en los lineamientos del marco de trabajo de riesgos de TI.

- Por medio de una consulta electrónica de extracción de datos en el sitio web del directorio de las páginas amarillas, se logró identificar 124 ferreterías ubicadas en la ciudad de Guatemala, a las cuales se les invitó a participar en la investigación por medio de una encuesta. El 20% correspondía a medianas empresas y todas utilizaban tecnología de la información.

- Se aplicó una muestra de expertos, a través de consultas con gerentes de negocio y gerentes de TI para obtener información de relaciones entre los procesos y los riesgos de activos informáticos.

- Se determinó el nivel de uso de tecnología de la información en la manera en la que hacen negocios, y que esta tecnología soporta o habilita a uno o varios procesos de negocio en las organizaciones objeto de estudio.

- Se determinó el nivel de apoyo que dan los activos informáticos a los procesos de negocio.

- Se identificaron factores de riesgo internos y externos que afectan los procesos por el uso de tecnología.

- Se evidenció la relación entre procesos de negocio y activos de TI y como los riesgos pueden producir interrupciones que ocasionen pérdidas financieras.

- Se generó un mapa de riesgo con base en el marco de trabajo de riesgos de TI, exponiendo el nivel de riesgo de activos informáticos, para exponer como el marco de trabajo de riesgos de TI y sus lineamientos, permiten conocer el

perfil de riesgo. Finalmente, se elaboró un plan de mitigación de riesgos y se efectuó el respectivo análisis financiero por medio de escenarios que dan a conocer las opciones que las organizaciones tienen para administrar su perfil de riesgo de activos informáticos.

4. MODELO DE RECOLECCIÓN DE DATOS DE RIESGOS DE ACTIVOS INFORMÁTICOS, MATRIZ DE ACTIVOS INFORMÁTICOS, MATRIZ DE PROCESOS DE NEGOCIO Y MATRIZ DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI)

El presente capítulo presenta los resultados del diseño de un modelo para la recolección de datos de los riesgos de los activos informáticos y la tecnología de la información utilizada para los negocios en medianas empresas ferreteras de la ciudad de Guatemala. Con los resultados obtenidos de la recolección de datos, se construyó la matriz de activos informáticos, matriz de procesos de negocio y la matriz de riesgos de tecnología de la información (TI); asimismo, se determinaron la ponderación de los factores de riesgo identificados.

Para el desarrollo de la matriz de riesgos de tecnologías de la información (TI), se aplicó el modelo RACI (por sus siglas en inglés, de Responsible, accountable, consulted, e informed) que corresponde a: Responsable, rendidor de cuentas, consultado e informado, como base para la rendición de cuentas.

De acuerdo con la investigación realizada, se determinó la forma en que las empresas catalogan el impacto financiero del riesgo de TI.

Tabla 6 - Escala de impacto financiero

En millones de Quetzales

Empresa	No Significativa	Baja	Media	Alta	Crítica
1	0.10	0.25	0.70	1.70	2.70
2	0.15	0.30	1.00	1.20	2.00
3	0.12	0.50	1.20	1.50	2.50
4	0.13	0.25	1.40	1.70	2.60
5	0.30	0.60	1.80	2.00	3.50
6	0.60	1.00	3.00	3.50	4.50
7	0.35	0.55	2.50	2.50	3.50
8	0.12	0.30	1.20	1.50	2.50
9	0.20	0.60	2.50	3.00	3.00
10	0.75	1.25	3.00	3.70	6.00
Promedio	0.28	0.56	1.83	2.23	3.28

Fuente: Elaboración propia, con base en información de la investigación realizada.

Los impactos financieros se consideran en el rango de 280 mil Quetzales hasta 3.28 millones de Quetzales.

Adicionalmente se complementó estos datos con entrevistas a varios profesionales de la tecnología de la información y gestores de riesgo de TI en 5 empresas de servicios especializados de soporte técnico. La intención fue obtener datos de referencia de la frecuencia de interrupciones de operación que la tecnología presenta en empresas medianas a las que ellos dan servicios. En este caso no era relevante el sector ya que la tecnología de la información no se sectoriza acorde al sector de industria, sino que es la misma a lo largo de todos los sectores y solo varía en función de capacidad técnica.

Tabla 7 - Frecuencia de interrupciones operacionales de Tecnología de la información

Frecuencia	Descripción
Muy Baja	Menos de una vez cada 3 o más años
Baja	Una vez cada 1 a 3 años
Media	Una vez cada 3 a 12 meses
Alta	Una vez cada 3 meses

Fuente: Elaboración propia, con base en información de la investigación realizada.

4.1 Modelo de recolección de datos de riesgos de tecnología de la información (TI)

El marco de trabajo RISK IT define que el modelo de recolección datos requiere de información respecto del entorno operativo, eventos de riesgo y factores de riesgo.

4.1.1 Matriz de Activos Informáticos

Esta matriz requiere de los siguientes datos:

- Activos informáticos en operación: Se refiere a los componentes tecnológicos que se usan para la operación de negocio.
- Responsable del Activo: Persona responsable del activo informático, quien proveyó de la información operativa relevante y es rendidor de cuentas del activo.
- Proceso de negocio al que soportan: Se refiere al proceso de negocio en el que se utilizan los activos informáticos
- Cantidad de incidentes de operación con base mensual: Se refiere a la cantidad de interrupciones de operación que sufrieron los activos informáticos con base mensual. Si no existe un sistema de conteo de

incidentes, se debe hacer bajo entrevistas a los participantes del proceso en el que participa el activo, con el fin de obtener un promedio sugerido.

- Duración de Incidentes: Indica la cantidad de horas en las que se tuvo interrupción a causa de incidentes, la cual finalmente cuantifica las horas en las que se tuvo interrupción operativa.

- Tiempo de uso en años: Cantidad de años de obsolescencia del activo informático.

- Cantidad de colaboradores que hacen uso del activo: Cantidad de personas que utilizan el activo informático, que ayudó a conocer el nivel de impacto operativo.

A continuación se presenta una ilustración de la matriz de activos informáticos, en vista de que la matriz completa contiene demasiados datos.

Tabla 8 - Matriz de activos informáticos (reducida)

Activo	**Servidor Local 1**	**Servidor Local 2**	**Servicio de e-mail**	**Sistema de Inventario**	**Sistema de Facturación**
Responsable del Activo	Juan S.	Juan S.	Pedro A.	Pedro S.	Pedro S.
Proceso de Negocio	Facturación Ventas Inventarios Compras Tesorería y Contabilidad	Planificación Estratégica Nóminas Control Interno Administración	Todos	Inventario Ventas Logística	Ventas Facturación Cuentas por cobrar
Incidentes promedio por mes	2	1	25	2	5
Duración de los	1	1.5	2	3	3

Activo	Servidor Local 1	Servidor Local 2	Servicio de e-mail	Sistema de Inventario	Sistema de Facturación
incidentes					
Tiempo de uso (Años)	2	1		3	3
Cantidad de usuarios	50	50	50	10	5
Factor de Riesgo	13.7	13.4	20.6	4.45	4.1

Fuente: Elaboración propia, con base en información de la investigación realizada.

Se identificaron cinco activos informáticos de interés para el desarrollo de la investigación; asimismo, se calculó el factor de riesgo, utilizando un promedio ponderado, con base en la definición de la necesidad organizacional. Los factores de riesgo afectan de manera diferente a cada organización por lo que se deben calcular para cada empresa cuando se desee aplicar este modelo.

Los valores ponderados para los factores de riesgo son los siguientes:

Tabla 9 - Ponderación de factores de riesgo

Factor de riesgo	Ponderación
Incidentes	30%
Duración	30%
Tiempo de uso	15%
Cantidad de usuarios	25%

Fuente: Elaboración propia, con base en información de la investigación realizada.

El cálculo de la ponderación del factor de riesgo se hizo de la manera siguiente:

Factor de riesgo = (Incidentes promedio por mes * peso de factor incidentes + Duración de incidentes * peso de factor de duración de incidentes + Tiempo de

uso del activo * peso del factor de uso de activo + Cantidad de usuarios * peso de factor cantidad de usuarios). Este dato fue de gran valor para definir los riesgos de mayor impacto en la matriz.

4.1.2 Matriz de procesos de negocio

La matriz de procesos de negocio se construyó con los siguientes datos:

- Proceso de Negocio: indica el proceso de negocio en análisis de riesgo por causa del uso de un activo informático dentro de la organización. Se listaron procesos en los cuales se hace uso de por lo menos un activo en algún punto del proceso, para garantizar que se hiciera un análisis de riesgo apropiado en las etapas posteriores del sistema de gestión de riesgos de TI.

- Responsable: Se refiere a la persona que responde por el proceso de negocio, quien generalmente entrega cuentas por el proceso. Fue de vital importancia tener claro quiénes eran los responsables de los procesos de negocio, para que, en el posterior análisis de riesgos, se tuviera oportunidad de consultar con ellos los impactos de las acciones de respuesta al riesgo, así como detalles de factores de riesgo que se identificaron debido a su experiencia.

- Tipo de información: Este dato referenció al tipo de registros que se almacenan o se manejan como parte de los procesos de negocio. Esto ayudo identificar la importancia del proceso en análisis, debido a que la información que se maneja en los procesos indica lo que pasaría si la información en un sistema o proceso es no confiable, ha sido alterada, mal manejada o no está disponible cuando se necesita. Todo lo anterior se consideró riesgo de interrupción de operación que resultaba en potencial pérdida de valor o pérdida financiera en algún momento determinado.

- Máximo Permitido de No disponibilidad (horas de negocio): El tiempo máximo en horas de negocio que la empresa está dispuesta a no contar con un proceso de negocio. Esté fue claro indicador de apetito de riesgo que también fue indicador de la importancia del proceso para la organización y resultó de utilidad para definir prioridad en ejecución de acciones de respuesta de riesgo en el plan de mitigación de riesgos. Mientras este valor es más cercano a cero, mayor es la prioridad del proceso ya que la organización no puede prescindir de este proceso por mucho tiempo.

- Clasificación de la información: los procesos de negocio hacen uso de información que se catalogará como: Publica, Uso de Negocio, Confidencial y Estrictamente Confidencial. Esta catalogación es acorde al capítulo 2

- Importancia/Ponderación en Operación: Ponderación del proceso de negocio, con base en lo que la alta dirección indicó.

- Activos Relacionados: Activos de TI que participaron en el proceso de negocio siendo analizado.

Tabla 10 - Matriz de procesos de negocio

Identificador de Proceso	P1	P2	P3	P4
Proceso de Negocio	Inventarios	Ventas	Tesorería y Contabilidad	Administración
Responsable	Mario Inventario	Jorge Negocios	Jorge Negocios	Jorge Negocios
Tipo de información	Reportes de Control de Inventario	Pedidos de Clientes Órdenes de Compra Clientes Pedidos de Inventario	Balances Generales Estados de Resultados Flujos de Efectivo Registros contables Registros de pago de Impuestos Cheques emitidos	indicadores de ejecución operativa Indicadores de eficiencia administrativa Indicadores de ejecución de presupuesto
Máxima indisponibilidad (horas)	16	8	24	40
Clasificación de la información	Confidencial	Confidencial	Confidencial	Uso de Negocio
Importancia / ponderación en operación	Alta	Crítica	Media	Baja
Activos relacionados	Servidor Local 1	Servidor Local 1	Servidor Local 1	Servidor Local 2
Factor de riesgo	9	11	7	4

Fuente: Elaboración propia, con base en información de la investigación realizada.

Al igual que con la matriz de activos informáticos, se calcularon factores de riesgo que sirvieron para la construcción de la matriz de riesgos de tecnología de la información (TI), que se presenta más adelante.

La ponderación se factores de riesgo se realizó de la siguiente manera:

Tabla 11 - Ponderación de factores de riesgo de procesos

Puntuación	1	2	3	4
No disponibilidad máxima	0 - 10	11 a 20	21 a 30	más de 30
Clasificación de la información	Pública	Uso de Negocio	Confidencial	Estrictamente confidencial
Importancia / Ponderación en Operación	Baja	Media	Alta	Crítica

Fuente: Elaboración propia, con base en información de la investigación realizada.

4.1.3 Matriz de riesgos de tecnología de la información (TI)

La matriz de riesgos de tecnología de la información (TI), se construyó con base en el modelo RACI (por sus siglas en inglés), que corresponde a: Responsable, rendidor de cuentas, consultado e informado, como base para la rendición de cuentas de los que deben velar por que las actividades se realicen con éxito. También se utilizaron los resultados de la ponderación de factores de riesgo de la matriz de activos informáticos y de la matriz de procesos. Se definió un nuevo factor de riesgo combinado, tomando el efecto del factor de riesgo ponderado del proceso de negocio, con el peso de los activos que participan en el proceso. El cálculo se hizo de la siguiente forma:

Factor de riesgo combinado = Factor ponderado de riesgo de proceso * (Sumatoria de Factores de riesgo de activos informáticos que participan en el proceso).

Esta matriz indica cual es el proceso con mayor nivel de exposición al riesgo por uso de tecnología. Los procesos con mayor puntuación se analizan posteriormente para ubicarlos en el mapa de riesgos y para definir acciones de respuesta al riesgo para reducir los niveles de exposición al riesgo.

Tabla 12 - Matriz de riesgo de activos informáticos

Identificador de proceso	**P1**	**P2**	**P3**	**P4**
Proceso de Negocio	Inventarios	Ventas	Tesorería y Contabilidad	Administración
Responsable	Mario I.	Jorge N.	Jorge N.	Jorge N.
Tipo de Información	Reportes de Control de Inventario	Pedidos de Clientes Órdenes de Compra Clientes Pedidos de Inventario	Balances Generales Estados de Resultados Flujos de Efectivo Registros contables Registros de pago de Impuestos Cheques emitidos	indicadores de ejecución operativa Indicadores de eficiencia administrativa Indicadores de ejecución de presupuesto
No disponibilidad máxima	16	8	24	40
Clasificación de la información	Confidencial	Confidencial	Confidencial	Uso de Negocio
Importancia	Alta	Crítica	Media	Baja

Identificador de proceso	P1	P2	P3	P4
Proceso de Negocio	Inventarios	Ventas	Tesorería y Contabilidad	Administración
Responsable	Mario I.	Jorge N.	Jorge N.	Jorge N.
Activos Relacionados	Servidor Local 1, Sistema de Inventarios, Red LAN, router internet, servicio de e-mail	Servidor Local 1, Sistema de Ventas, Red LAN, router internet, servicio de e-mail	Servidor Local 1, Sistema de Tesorería, Red LAN, router internet, servicio de e-mail	Servidor Local 1, Sistema de Administración, Red LAN, router internet, servicio de e-mail
Factor riesgo combinado	349	422	269	154

Fuente: Elaboración propia, con base en información de la investigación realizada.

Del análisis anterior se evidencia que el proceso de ventas es el proceso más expuesto al riesgo por uso de tecnología de la información. El análisis que se desarrolló toma en cuenta todos los activos que participan en la ejecución del proceso de ventas para identificar cuáles son los elementos que provocan que los activos estén con elevado nivel de riesgo.

5. MARCO DE TRABAJO RISK IT (RIESGO DE TECNOLOGÍA DE LA INFORMACIÓN), PARA LA GESTION DE RIESGOS DE ACTIVOS INFORMÁTICOS EN MEDIANAS EMPRESAS FERRETERAS

El presente capítulo presenta los resultados de la investigación relacionados con el marco de trabajo RISK IT (Riesgo de Tecnología de la Información), para la gestión de riesgo de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala.

Los resultados incluyen el análisis de la matriz de evaluación de riesgos de activos informáticos, el mapa de apetito de riesgo de TI, definición del plan de mitigación, análisis del impacto financiero y el análisis a través de escenarios optimista y pesimista.

5.1 Análisis en la matriz de riesgo de activos informáticos

En la matriz de riesgos de activos informáticos del capítulo anterior, se evidenció que el proceso de ventas es el proceso con un nivel crítico de exposición al riesgo y que los activos que lo posicionan con este perfil son: Servidor Local 1, Sistema de Ventas, Red LAN, router internet y servicio de e-mail.

El proceso de inventarios tiene un nivel alto de exposición al riesgo. Después sigue el proceso de tesorería y contabilidad con un nivel de riesgo medio, y la administración con un nivel de riesgo bajo.

Es importante comentar que se detectó que varios activos informáticos soportan más de un proceso, por ejemplo, el servidor local 1, interviene en los cuatro procesos que se analizaron.

Con base en el marco de trabajo de riesgos de TI y la tabla de escala de impacto financiero procedió a identificar cuales factores de riesgo hacen que estos activos sean riesgosos desde un punto de vista técnico operacional.

Se listaron los activos que participaron en los procesos de negocio y se desglosaron los posibles impactos que se identificaron. Con esto, se logró definir las escalas de frecuencia de ocurrencia de los ítems de riesgo y la escala de impacto financiero en la que se ubicaban.

Tabla 13 - Análisis de riesgos en procesos de ventas por uso de tecnología de la información

ID	Ítem de riesgo	Frecuencia (Mensual)	Escala de impacto financiero
	Servidor Local 1		
R1	Incidentes recurrentes por obsolescencia	Alta	Crítico
R2	Incidentes por calidad de componentes	Media	Crítico
R3	Incidentes por capacidad insuficiente para procesamiento de datos	Media	Crítico
	Sistema de Ventas / Inventario / Tesorería / Administración		
R4	Interrupciones por servidor	Media	Alto
R5	Interrupciones por no disponibilidad de sistema	Muy Baja	Alto
	Red LAN		
R6	Interrupciones por saturación	Baja	Medio
R7	Interrupciones por cortes de energía eléctrica	Baja	Medio
	Router Internet		
R8	Lentitud por falta de capacidad de procesamiento de tráfico	Alta	Medio
	Servicio de e-mail		
R9	Interrupciones por no disponibilidad de servicio	Muy Baja	No significativo
R10	Interrupciones por actualizaciones del servicio no programadas	Baja	No significativo

Fuente: Elaboración propia, con base en información de la investigación realizada.

La columna ID, fue añadida para facilidad de lectura en las secciones futuras, en donde el primer ítem de riesgo tiene asignado el identificador R1, el segundo tiene el identificador R2, y así sucesivamente.

5.2 Escala de impacto financiero

Luego de definir la matriz de riesgos de activos informáticos, se procedió a la elaboración del mapa de apetito de riesgo con base en el marco de trabajo de riesgos de TI, con el fin de conocer el perfil de riesgo de la configuración de activos informáticos.

El impacto financiero se calculó como un rango, el cual se obtuvo de la encuesta inicialmente enviada a las empresas medianas del sector ferretero que participaron de la encuesta.

La escala de impacto financiero resultante fue con base en los promedios de los datos provistos en la encuesta, con redondeo al ciento más cercano para mejor visibilidad:

Tabla 14 - Escala de impacto financiero

Categoría	Impacto en GTQ
No Significativa	0 a 300,000
Baja	301,000 a 600,000
Media	601,000 a 2,000,000
Alta	2,000,001 a 2,500,000
Crítica	2,500,001 a 3,500,000

Fuente: Elaboración propia, con base en información de la investigación realizada.

Estos valores son la base para proyectar pérdidas en el análisis de escenarios, en donde el límite inferior del rango es el escenario optimista y el límite superior representa el escenario pesimista.

5.3 Mapa de apetito de riesgo

El mapa de apetito de riesgo sirvió de herramienta visual para conocer el nivel de apetito de riesgo con base en los resultados de la matriz de riesgo en procesos de ventas por uso de tecnología de la información:

Tabla 15 - Mapa de apetito de riesgo

Impacto Financiero					
	Crítica			R2, R3	R1
	Alta	R5		R4	
	Media		R6, R7		R8
	Baja				
	No Significativa	R9	R10		
		Muy Baja	Baja	Media	Alta
		Frecuencia			

Fuente: Elaboración propia, con base en información de la investigación realizada.

Los colores en el mapa representaron bandas de apetito de riesgo que tienen el siguiente significado:

- Azul: No significativo, es decir, la ignora el nivel de riesgo. NO necesariamente habrá reacción a eventos de riesgo.

- Verde: Aceptable, la empresa asume el riesgo. Se podría reaccionar a eventos de riesgo con prioridad baja.

- Amarillo: Inaceptable, la empresa no asumirá riesgo y reaccionará a los ítems de riesgo con prioridad media en el corto-mediano plazo.

- Rojo: Estrictamente inaceptable, la empresa no tolerará el nivel de riesgo y reaccionará en el corto plazo con prioridad alta a los eventos de riesgo.

5.4 Plan de mitigación de riesgos de activos informáticos

El plan de mitigación contiene un resumen ejecutivo de los riesgos presentados en la matriz de riesgos de tecnología de la información, la escala de impacto financiero, el mapa de apetito al riesgo y las acciones de respuesta al riesgo, incluyendo el análisis económico financiero.

5.4.1 Priorización de ítems de riesgo

La priorización de los ítems de riesgo se realiza conforme a su posición en el mapa de apetito de riesgo, para definir las acciones que se deben tomar para mitigar el riesgo. Esto se hace como paso previo para definir acciones de respuesta de manera secuencial, buscando atender con prioridad ítems de riesgo que generarían mayor pérdida financiera.

Tabla 16 - Priorización de Ítems de riesgos

ID	Activo Informático	Ítem de riesgo	Prioridad
R1	Servidor Local 1	Incidentes recurrentes por obsolescencia	1
R2		Incidentes por calidad de componentes	1
R3		Incidentes por capacidad insuficiente para procesamiento de datos	1
R4	Sistema de Ventas / Inventario / Tesorería / Administración	Interrupciones por servidor	2
R5		Interrupciones por no disponibilidad de sistema	2
R6	Red de área local	Interrupciones por saturación	3
R7		Interrupciones por cortes de energía eléctrica	3
R8	Router Internet	Lentitud por falta de capacidad de procesamiento de tráfico	1
R9	Servicio de e-mail	Interrupciones por no disponibilidad de servicio	3
R10		Interrupciones por actualizaciones del servicio no programadas	4

Fuente: Elaboración propia, con base en información de la investigación realizada.

5.4.2 Proyección de pérdidas por materialización de riesgos

Las pérdidas financieras proyectadas se obtuvieron multiplicando la ocurrencia anual de los ítems de riesgo por los límites inferior y superior de la escala de impacto financiero.

Tabla 17 - Análisis de impacto financiero de los ítems de riesgo

ID	Activo Informático	Ocurrencia Anual	Escenario Optimista GTQ	Impacto Pesimista GTQ
R1	Servidor Local 1	2	5,000,002	7,000,000
R2		0.5	1,250,001	1,750,000
R3		0.5	1,250,001	1,750,000
R4	Sistema de Ventas / Inventario / Tesorería / Administración	0.5	1,000,001	1,250,000
R5		0.1	200,000	250,000
R6	Red de área local	0.2	120,200	400,000
R7		0.2	120,200	400,000
R8	Router Internet	1	601,000	2,000,000
R9	Servicio de e-mail	0.1	-	30,000
R10		0.1	-	30,000
	TOTAL		**9,541,405**	**14,860,000**

Fuente: Elaboración propia, con base en información de la investigación realizada.

El impacto financiero proyectado total anual por los ítems de riesgo en las bandas fue resultado de la suma de cada uno de los valores de cada ítem de riesgo, tanto en el escenario optimista, como en el escenario pesimista:

Tabla 18 - Pérdida total proyectada

Banda	Ítems de riesgo presentes	Escenario Optimista GTQ	Escenario Pesimista GTQ
No significativa	R9	-	30,000
Aceptable	R6, R7, R10	240,400	830,000
Inaceptable	R4, R5	1,200,001	1,500,000
Estrictamente inaceptable	R1, R2, R3, R8	8,101,004	12,500,000
Total		**9,541,405**	**14,860,000**

Fuente: Elaboración propia, con base en información de la investigación realizada.

El interés se centra específicamente en los ítems de las bandas inaceptable y estrictamente inaceptable, los cuales sumaron: GTQ 9.3 millones en el escenario optimista y GTQ14 millones en el escenario pesimista.

5.4.3 Estados de resultados pro forma

Una vez identificadas las cuentas del estado de resultados en donde las pérdidas impactarían, se procede a la elaboración de estados de resultados pro forma base, así como para el escenario optimista como el pesimista.

Tabla 19 - Estado de resultados base

En GTQ

	2017	2018	2019
Ventas	31,485,171	33,059,430	35,042,996
Costo de Ventas	-14,801,426	-19,941,498	-22,138,573
Utilidad bruta	**16,683,745**	**13,117,932**	**12,904,423**
Gastos administrativos	-896,381	-941,200	-988,260
Utilidad en Operaciones	**15,787,364**	**12,176,732**	**11,916,163**
Gastos financieros	-235,465	-150,763	-50,867
Otros Ingresos/Egresos	-145,744	-107,512	-68,580
Utilidad Antes de Impuestos	**15,406,155**	**11,918,457**	**11,796,716**
Impuestos (25%)	-3,851,539	-2,979,614	-2,949,179
Utilidad después de Impuestos	**11,554,616**	**8,938,843**	**8,847,537**
Margen de ganancia sobre ventas	**36.7%**	**27.0%**	**25.2%**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Para el estado de resultados de cada uno de los escenarios, se aplica el análisis de impacto financiero de los ítems de riesgo. Estos son los resultados que se presentan a la administración, para integrar la gestión de riesgos a la toma de decisiones, para definir un plan de mitigación

Tabla 20 – Impacto en cuentas del estado de resultados pro forma, en el escenario pesimista

Proceso	Ventas	Inventario	Tesorería	Administración
Cuenta en estado de resultados	Ventas	Ventas	Gastos de Admón.	Gastos de Admón.
R1	40% -2,800,000	40% -2,800,000	10% - 700,000	10% - 700,000
R2, R3	40% -1,400,000	40% -1,400,000	10% - 350,000	10% - 350,000
R8	25% -500,000	25% - 500,000	25% - 500,000	25% - 500,000
R4	30% - 375,000	30% - 375,000	15% - 187,500	25% - 312,500
R5	30% - 75,000	30% - 75,000	15% - 37,500	25% - 62,500
Total	**-5,150,000**	**-5,150,000**	**- 1,775,000**	**- 1,925,000**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Los porcentajes mostrados son la afectación de las cuentas del estado de resultados. Ese factor se asigna con apoyo de los gestores de procesos y la dirección de TI. Se define acorde a los factores tanto internos como externos de exposición al riesgo, como lo establece el marco de trabajo de riesgos de TI. No es posible asignar un factor a todo el sector objeto de estudio, en vista de que las necesidades organizacionales son específicas para cada empresa.

Tabla 21 – Impacto en cuentas del estado de resultados pro forma, en el escenario optimista

Proceso	Ventas	Inventario	Tesorería	Administración
Cuenta en estado de resultados	Ventas	Ventas	Gastos de Admón.	Gastos de Admón.
R1	40% - 2,000,001	40% -2,000,001	10% - 500,000	10% - 500,000
R2, R3	40% - 1,000,000	40% -1,000,000	10% - 250,000	10% - 250,000
R8	25% - 150,250	25% - 150,250	25% - 150,250	25% - 150,250
R4	30% - 300,000	30% - 300,000	15% - 150,000	25% - 250,000
R5	30% - 60,000	30% - 60,000	15% - 30,000	25% - 50,000
Total	**- 3,510,251**	**- 3,510,251**	**- 1,080,250**	**- 1,200,250**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Con base en el impacto determinado de los ítems de riesgo inaceptable y estrictamente inaceptable, en cuentas de resultados, se elabora el estado de resultados pro forma para cada escenario.

5.4.3.1 Estado de resultados pro forma, escenario optimista

El estado de resultados pro forma del escenario optimista, es el siguiente:

Tabla 22 - Estado de resultados pro forma, escenario optimista

En GTQ

	2017	2018	2019
Ventas	24,464,669	26,038,927	28,022,493
Costo de Ventas	-14,801,426	-19,941,498	-22,138,573
Utilidad Bruta	**9,663,242**	**6,097,429**	**5,883,920**
Gastos Administrativos	-3,176,882	-3,221,701	-3,268,761
Utilidad en Operaciones	**6,486,361**	**2,875,729**	**2,615,160**
Gastos Financieros	-235,465	-150,763	-50,867
Balance de otros Ingresos/Egresos	-145,744	-107,512	-68,580
Utilidad Antes de Impuestos	**6,105,152**	**2,617,454**	**2,495,713**
Impuestos (25%)	-1,526,288	-654,363	-623,928
Utilidad después de Impuestos	**4,578,864**	**1,963,090**	**1,871,785**
Margen de ganancia sobre ventas	**18.7%**	**7.5%**	**6.7%**
Pérdida de utilidad	**6,975,753**	**6,975,753**	**6,975,753**
% de pérdida de utilidad	**60.4%**	**78.0%**	**78.8%**

Fuente: Elaboración propia, con base en información de la investigación realizada.

La pérdida de utilidad se calcula por diferencia, con respecto al estado de resultados base. Por ejemplo, la utilidad proyectada en el estado de resultados base para el año 2017 es de GTQ 11.55 millones y la utilidad proyectada para ese mismo año en el estado de resultados del escenario optimista es de GTQ 4.58 millones, de donde resulta una diferencia de GTQ 6.97 millones. Esta diferencia o pérdida de utilidad, equivale al 60.4% de la utilidad proyectada para el estado de resultados base, aunque la mayor pérdida de utilidad ocurre en la proyección del año 2018, con 88.1%.

5.4.3.2 Estado de resultados pro forma con escenario pesimista

El escenario pesimista representó el peor de los casos y fue necesario calcularlo, para representar los niveles de impacto que se pueden sufrir por no mitigar los riesgos de activos informáticos.

Tabla 23 - Estado de resultados pro forma, escenario pesimista
En GTQ

	2017	2018	2019
Ventas	21,185,171	23,789,430	24,742,996
Costo de Ventas	-14,801,426	-19,941,498	-22,138,573
Utilidad Bruta	**6,383,745**	**3,847,932**	**2,604,423**
Gastos Administrativos	-4,596,381	-4,641,200	-4,688,260
Utilidad en Operaciones	**1,787,364**	**-793,268**	**-2,083,837**
Gastos Financieros	-235,465	-150,763	-50,867
Balance de otros Ingresos/Egresos	-145,744	-107,512	-68,580
Utilidad Antes de Impuestos	**1,406,155**	**-1,051,543**	**-2,203,284**
Impuestos (25%)	-351,539	262,886	550,821
Utilidad después de Impuestos	**1,054,616**	**-788,657**	**-1,652,463**
Margen de ganancia sobre ventas	**5.0%**	**-3.3%**	**-6.7%**
Pérdida de utilidad	**10,500,000**	**9,727,500**	**10,500,000**
% de pérdida de utilidad	**90.9%**	**108.8%**	**118.7%**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Para el año 2017, la pérdida de utilidad proyectada es de GTQ 10.5 millones, equivalente al 90.9% de la utilidad proyectada para ese mismo año en el estado de resultados base.

Esta información es de mucho valor para discutir con la alta dirección apoyar la toma de decisiones para la puesta en marcha de las actividades de respuesta al riesgo.

5.4.4 Definición de actividades de respuesta al riesgo

Las actividades de respuesta al riesgo se definieron con base en los ítems de riesgo que representan la mayor pérdida financiera proyectada. Estos fueron: R4, R5 para la banda de apetito de riesgo inaceptable y R1, R2, R3 y R8 para la banda de apetito de riesgo estrictamente inaceptable.

Para los ítems en la banda estrictamente inaceptable se definieron las siguientes acciones con el apoyo de los encargados de TI:

Tabla 24 - Actividades de respuesta al riesgo para ítems en la banda de estrictamente inaceptable

ID	R1	R2	R3	R8
Activo Informático	Servidor Local 1			Router Internet
Ítem de riesgo	Incidentes recurrentes por obsolescencia	Incidentes por calidad de componentes	Incidentes por capacidad insuficiente para procesamiento de datos	Lentitud por falta de capacidad de procesamiento de tráfico
Prioridad	1	1	1	1

ID	R1	R2	R3	R8
Acciones	Renovación tecnológica de servidor	Evaluación comparativa de servidores más utilizados en la industria del sector ferretero y/o sector de medianas empresas con volumen similar de procesamiento de datos.		Renovación tecnológica. Evaluación comparativa de routers más utilizados en la industria del sector ferretero y/o sector de medianas empresas con volumen similar de procesamiento de datos.

Fuente: Elaboración propia, con base en información de la investigación realizada.

Tabla 25 - Actividades de respuesta al riesgo para ítems en la banda de inaceptable

ID	R4	R5
Activo Informático	Sistema de Ventas / Inventario / Tesorería / Administración	
Ítem de riesgo	Interrupciones por servidor	Interrupciones por no disponibilidad de sistema
Prioridad	2	2
Acciones	Renovación tecnológica de servidor. Migración a versión más moderna de sistema.	Mantenimientos programados en horario no laboral y con políticas de gestión de cambios

Fuente: Elaboración propia, con base en información de la investigación realizada.

Las actividades de respuesta al riesgo se discuten con la dirección de TI o los encargados de los activos informáticos para prever actividades para para reducir el nivel de riesgo.

Se busca evaluar y establecer acciones que no necesariamente representen costo a la organización. Es importante hacer ver a la dirección de TI que existen actividades de respuesta al riesgo que se pueden limitar a un cambio en políticas internas o promoción de la cultura de riesgo que no necesariamente requieren de inversión.

5.4.5 Análisis financiero de las actividades de respuesta al riesgo

Con las acciones definidas se procede a calcular costos preliminares de inversiones requeridas. En los casos en los que se requiera de inversiones para reemplazo de activos, se evalúa el apalancamiento tecnológico para consolidar esfuerzos y costos.

Tabla 26 - Análisis preliminar de costos de actividades de respuesta al riesgo

Acciones en la banda de estrictamente inaceptable				
ID	**R1**	**R2**	**R3**	**R8**
Activo Informático	Servidor Local 1			Router Internet
Acciones	Renovación tecnológica de servidor	Evaluación comparativa de servidores más utilizados en la industria del sector ferretero y/o sector de medianas empresas con volumen similar de procesamiento de datos.		Renovación tecnológica. Evaluación comparativa de routers más utilizados en la industria del sector ferretero y/o sector de medianas empresas con volumen similar de procesamiento de datos.

Acciones en la banda de estrictamente inaceptable				
ID	**R1**	**R2**	**R3**	**R8**
Costo Sugerido en GTQ	40,000		-	8,000
Total GTQ				48,000

Acciones en la banda de inaceptable		
ID	**R4**	**R5**
Activo Informático	Sistema de Ventas / Inventario / Tesorería / Administración	
Acciones	Renovación tecnológica de servidor. Migración a versión más moderna de sistema.	Mantenimientos programados en horario no laboral y con políticas de gestión de cambios
Costo Sugerido	20,000.00	-
Total		20,000.00

Fuente: Elaboración propia, con base en información de la investigación realizada.

Se logró apreciar en el análisis económico, que en los sistemas de ventas, inventario, tesorería y administración, es necesario invertir para renovar y mejorar el nivel de tecnología. Debido a que los sistemas están en servidores separados, hay dos posibles líneas de acción:

Continuar con servidores separados: Lo cual representa costo mayor, pero menor riesgo consolidado de interrupción de procesos, en vista de que la falla de un solo servidor, afecta solamente el proceso alojado en el servidor que presenta falla.

Servidor único con redundancia y mayor capacidad de procesamiento de datos: Se planteó invertir en dos servidores para tener redundancia.

La propuesta se sugirió así, de modo que mientras se opere en el servidor secundario por fallas en el primario, se ofrezca servicio a procesos en menor nivel

comparado con el primario, es decir ofrecer 70%-80% de nivel de servicio respecto del servidor primario.

La propuesta busca reducir costos de la acción de respuesta al riesgo.

En el caso de la otra actividad que representó adquisición de activos informáticos se manejó de la misma manera, pero sin propuesta de redundancia.

Tabla 27 - Análisis de impacto financiero de ítems de riesgo en la banda de estrictamente inaceptable en cuentas de estado de resultados

Proceso	Cuenta	Efecto de R1		Efecto de R2, R3		Efecto de R8	
Ventas	Ventas	40%	16,000	40%	-	25%	2,000
Inventario	Ventas	40%	19,200	40%	-	25%	2,000
Tesorería	Gastos de Admón.	10%	-	10%	-	25%	2,000
Administración	Gastos de Admón.	10%	-	10%	-	25%	2,000
Total							**43,200**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Tabla 28 - Análisis de impacto financiero de ítems de riesgo en banda inaceptable en cuentas de estado de resultados

Proceso	Cuenta ER	R4		R5	
Ventas	Ventas	40%	8,000	25%	-
Inventario	Ventas	40%	8,000	25%	-
Tesorería	Gastos de Admón.	10%	2,000	25%	-
Administración	Gastos de Admón.	10%	2,000	25%	-
Total					**20,000**

Fuente: Elaboración propia, con base en información de la investigación realizada.

El desglose de impacto financiero del costo de las actividades de respuesta al riesgo, para cada uno de los ítems de riesgo en las bandas de estrictamente inaceptable e inaceptable se realiza en conjunto con los gestores de procesos y la dirección de TI y encargados de procesos.

La reunión al ser multidisciplinaria, logra promover la cultura de riesgo, para que todos los participantes comprendan la importancia de mitigar niveles de exposición al riesgo, para evitar pérdidas financieras.

5.4.5.1 Caso de negocio de actividades de respuesta al riesgo

Con los costos preliminares, se procede a calcular los flujos de efectivo de las inversiones a ejecutar, para luego presentarlos a la alta dirección.

Tabla 29 - Flujo de efectivo de actividades de respuesta al riesgo

En GTQ

Concepto	2017	2018	2019	2020
Ingresos	**1,500**	**-**	**-**	**-**
Venta servidor	1,500	-	-	-
Valor de Rescate	-	-	-	-
Egresos	**-58,000**	**-5,000**	**-5,000**	**-20,000**
Servidor primario	-28,000	-	-	-
Servidor secundario	-12,000	-	-	-
Router internet	-8,000	-	-	-
Licencias de Sistemas (Ventas, inventarios, tesorería, administración)	-10,000	-5,000	-5,000	-20,000
Utilidad neta	**-56,500**	**-5,000**	**-5,000**	**-20,000**
Impuestos 25%	-14,125	-1,250	-1,250	-5,000
Flujo de Caja	**-70,625**	**-6,250**	**-6,250**	**-25,000**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Se presentó la opción de servidor primario y secundario para redundancia de infraestructura y alta disponibilidad de servicio. Las licencias del sistema se planificaron como compras separadas por módulos, con desembolsos menores en años siguientes.

6. GESTIÓN DE RIESGOS DE ACTIVOS INFORMÁTICOS, POST MITIGACIÓN

Posteriormente a ejecutar las evaluaciones de riesgo y de impactos financieros, se procede a evaluar las proyecciones de niveles de riesgo en la etapa de riesgos mitigados. Esto requiere llevar a cabo nuevamente la gestión de riesgos de activos informáticos con base en el marco de trabajo RISK IT (Riesgo de Tecnología de la Información), pero con nuevos datos de exposición al riesgo, más bajos.

6.1 Proyección de nivel de riesgo

Para comenzar, se solicita a un gestor de riesgos de TI de una empresa transnacional que revisare las actividades de respuesta al riesgo para que indique cuanto podría reducirse el riesgo con estas actividades. El principal factor que debe bajar de escala es la ocurrencia anual del riesgo identificado, para medir su incidencia en las proyecciones optimista y pesimista.

Los efectos que se esperan, son la reducción directa del posicionamiento en la escala de impacto financiero para los escenarios pesimista y optimista, con base en las proyecciones de reducción de niveles de exposición al riesgo que se plantearon, buscando un acercamiento conservador, en donde los niveles de exposición se reduzcan aproximadamente en un 75%, que es el indicado, según los gerentes de gestión de riesgos de TI para actualización de tecnología de activos informáticos. Se plantea la reducción de incidencias anuales de hasta 90%, pero con enfoque conservador se sugiere aproximadamente el 75%.

Tabla 30 - Matriz de activos informáticos post mitigación de exposición al riesgo

ID	Activo informático	Ocurrencia anual	Escenario optimista	Impacto pesimista
R1	Servidor Local 1	0.25	625,000	875,000
R2		0.25	625,000	875,000
R3		0.25	625,000	875,000
R4	Sistema de Ventas / Inventario / Tesorería / Administración	0.25	500,000	625,000
R5		0.05	100,000	125,000
R6	Red de área local	0.25	150,250	500,000
R7		0.05	30,050	100,000
R8	Router Internet	0.25	150,250	500,000
R9	Servicio de e-mail	0.05	-	15,000
R10		0.05	-	15,000

Fuente: Elaboración propia, con base en información de la investigación realizada.

6.2 Mapa de riesgo en etapa post mitigación

El mapa de apetito de riesgo también debe ser recalculado.

Tabla 31 - Mapa de apetito de riesgo en etapa de post mitigación

Impacto Financiero					
	Crítica				
	Alta				
	Media	**R7**	**R2, R4**		
	Baja	**R5, R6**	**R1, R3, R8**		
	No Significativo	**R9, R10**			
		Muy Baja	Baja	Media	Alta
		Frecuencia			

Fuente: Elaboración propia, con base en información de la investigación realizada.

Se puede apreciar en el mapa de apetito de riesgo, que los ítems de riesgo cambian su posición en las bandas de apetito.

R1, R2, R3 y R8 cambian de la banda estrictamente inaceptable a la banda aceptable.

R4 y R5 quedaron también en la banda aceptable.

R6 y R7, a pesar de que no tuvieron cambio de banda, si bajaron su ocurrencia anual y su impacto financiero.

R10 cambio de la banda aceptable a la banda no significativa.

Finalmente, R9 no sufrió cambio de banda, en vista de que estaba en la banda inferior.

6.3 Pérdidas proyectadas post mitigación

La pérdida total calculada queda de la siguiente manera:

Tabla 32 - Pérdidas proyectadas para escenarios optimista y pesimista en etapa de post mitigación de riesgos de activos informáticos

Banda	Ítems de riesgo presentes	Escenario optimista GTQ	Escenario pesimista GTQ
No significativa	R9	-	15,000
Aceptable	R6, R7, R10	180,300	615,000
Inaceptable	R4, R5	600,000	750,000
Estrictamente inaceptable	R1, R2, R3, R8	2,025,251	3,125,000
Total		**2,805,551**	**4,505,000**

Fuente: Elaboración propia, con base en información de la investigación realizada.

Las pérdidas de los escenarios se vieron reducidas en aproximadamente un 70%.

6.4 Estado de resultados pro forma post mitigación

Finalmente se presentan los estados de resultados proyectados como evidencia de la evolución positiva del impacto de los riesgos hasta la etapa de mitigación.

Es fundamental dar a conocer el impacto financiero, con base en estados de resultados pro forma base y de los escenarios propuestos. También es importante consolidad los resultados por etapas, base, previo a la mitigación de riesgos y en la etapa post mitigación, para que se pueda apreciar la creación de valor a través de la eficiente gestión de riesgos de tecnología de la información, (TI) con base en el marco de trabajo RISK IT (Riesgo de Tecnología de la Información).

Tabla 33 - Resumen de escenarios de etapas de gestión previo a mitigación y post mitigación de riesgos de activos informáticos

Etapa	Escenario	Pérdida de utilidad		
		2017	**2018**	**2019**
Previo a mitigación	Pesimista	90.9%	108.8%	-118.7%
	Optimista	60.4%	78.0%	78.8%
Post Mitigación	Pesimista	25.2%	32.5%	32.8%
	Optimista	17%	18.2%	21.2%

Fuente: Elaboración propia, con base en información de la investigación realizada.

Tabla 34 - Estado de resultados pro forma, escenario pesimista, etapa de post mitigación de riesgos de activos informáticos

En GTQ

	2017	**2018**	**2019**
Ventas	28,685,171	30,259,430	32,242,996
Costo de Ventas	-14,801,426	-19,941,498	-22,138,573
Utilidad bruta	**13,883,745**	**10,317,932**	**10,104,423**
Gastos administrativos	-1,971,381	-2,016,200	-2,063,260
Utilidad en Operaciones	**11,912,364**	**8,301,732**	**8,041,163**
Gastos financieros	-235,465	-150,763	-50,867
Otros ingresos/egresos	-145,744	-107,512	-68,580
Utilidad Antes de Impuestos	**11,531,155**	**8,043,457**	**7,921,716**
Impuestos (25%)	-2,882,789	-2,010,864	-1,980,429
Utilidad después de Impuestos	**8,648,366**	**6,032,593**	**5,941,287**
Margen de ganancia sobre ventas	**30.1%**	**19.9%**	**18.4%**
Pérdida de utilidad	**2,906,250**	**10,406,250**	**2,906,250**
% De pérdida de utilidad	**25.2%**	**63.3%**	**32.8%**

Fuente: Elaboración propia, con base en información de la investigación realizada.

En el año 2017, en el escenario pesimista, en la etapa de post mitigación, las pérdidas de utilidad logran reducirse en 65.7 puntos porcentuales. De 90.9%, se

reducen a 25.2%, en el año 2017. La utilidad del año base de GTQ 11.55 millones, se reduce a GTQ 58.65 millones (Reducción de pérdida de GTQ 2.90 millones).

Tabla 35 – Estado de resultados pro forma, escenario optimista, etapa post mitigación de riesgos de activos informáticos

En GTQ

	2017	**2018**	**2019**
Ventas	29,550,046	31,124,304	33,107,870
Costo de Ventas	-14,801,426	-19,941,498	-22,138,573
Utilidad Bruta	**14,748,619**	**11,182,806**	**10,969,297**
Gastos Administrativos	-1,586,506	-1,631,325	-1,678,385
Utilidad en Operaciones	**13,162,113**	**9,551,481**	**9,290,912**
Gastos Financieros	-235,465	-150,763	-50,867
Otros Ingresos/Egresos	-145,744	-107,512	-68,580
Utilidad Antes de Impuestos	**12,780,904**	**9,293,206**	**9,171,465**
Impuestos (25%)	-3,195,226	-2,323,302	-2,292,866
Utilidad después de Impuestos	**9,585,678**	**7,313,592**	**6,972,286**
Margen de ganancia sobre ventas	**32.4%**	**23.5%**	**21.1%**
Pérdida de utilidad	**1,968,938**	**9,125,251**	**1,875,251**
% de pérdida de utilidad	**17.0%**	**55.5%**	**21.2%**

Fuente: Elaboración propia, con base en información de la investigación realizada.

En el año 2017, en el escenario optimista, en la etapa de post mitigación, las pérdidas de utilidad logran reducirse en 43.4 puntos porcentuales. De 60.4%, se reducen a 17.0%, en el año 2017. La utilidad del año base de GTQ 11.55 millones, se reduce a GTQ 9.59 millones (Reducción de pérdida de GTQ 1.96 millones).

6.5 Resumen ejecutivo

Toda la información debe consolidarse como un resumen ejecutivo para la alta dirección. El contenido sugerido del resumen ejecutivo, con base en el sistema de gestión propuesto debe incluir los siguientes aspectos:

- Matriz de riegos
- Mapa de riesgos
  - Situación pre gestión de riesgos
  - Proyección post mitigación
- Resumen de actividades de respuesta al riesgo
  - Caso de negocio
- Estados de resultados pro forma
- Resumen de análisis de utilidad en etapas de gestión de riesgo
- Anexos
  - Matriz de riesgo de activos
  - Matriz de riesgos de procesos de negocio

CONCLUSIONES

1. Los resultados de la investigación realizada permitieron comprobar la hipótesis formulada, en vista de que la propuesta del sistema de gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información), en las medianas empresas ferreteras de la ciudad de Guatemala, permitió integrar la gestión de riesgos a la toma de decisiones; la construcción de la matriz de riesgo de activos informáticos, la matriz de procesos de negocio y la ponderación de factores de riesgo; la creación del mapa de apetito al riesgo de TI; la definición de un plan de mitigación de riesgos; el análisis del impacto en pérdidas financieras por materialización de riesgos; el análisis de escenarios optimista y pesimista; y, la definición de actividades de mitigación para la respuesta a los riesgos de activos informáticos catalogados en un nivel inaceptable y estrictamente inaceptable.

2. El modelo de recolección de datos de riesgos de tecnología de la información (TI), permitió generar la matriz de activos informáticos, la ponderación de factores de riesgo, la matriz de procesos de negocio, y la ponderación de factores de riesgo de procesos. En la matriz de activos informáticos se determinaron cinco activos informáticos de interés para la investigación: Servidor 1, servidor 2, servicio de e-mail (correo electrónico), sistema de inventario y sistema de facturación. En procesos de negocio el riesgo de activos informáticos es crítico en ventas, alto en inventarios, medio en tesorería y contabilidad y bajo en actividades de administración.

3. En el mapa de apetito al riesgo en procesos de ventas, se detectó que los ítems de riesgo estrictamente inaceptables, son: Incidentes recurrentes por obsolescencia, incidentes por calidad de componentes e incidentes por capacidad insuficiente para procesamiento de datos y la lentitud por falta de

capacidad de procesamiento de tráfico. Los riesgos inaceptables, son: Interrupciones por servidor e interrupciones por no disponibilidad de sistema.

4. La proyección de pérdidas por materialización de riesgos de activos informáticos, en el año 2017, se cuantificó en GTQ 9,541,405 en el escenario optimista y GTQ 14,860,000 en el escenario pesimista. El impacto en cuentas del estado de resultados afecta ventas, inventarios y gastos de administración.

5. En el escenario optimista del año 2017, se proyecta una pérdida de utilidad de GTQ 6.97 millones con respecto a la utilidad de GTQ 11.55 millones en el estado de resultados pro forma base (La utilidad en el estado de resultados pro forma optimista es de GTQ 4.58 millones). En el escenario pesimista, la pérdida de utilidad proyectada es de GTQ 10.5 millones, en vista de que la utilidad en este escenario es de solamente GTQ 1.05 millones.

6. Luego de la definición de actividades de respuesta al riesgo, el análisis de gestión de riesgos de activos informáticos, post mitigación, determinó cambios radicales en el mapa de apetito de riesgo. Las pérdidas proyectadas en el escenarios optimista se reducen drásticamente a GTQ.2,805,551 y en el escenario pesimista a GTQ.4,505,000.

RECOMENDACIONES

1. Los resultados satisfactorios de la investigación realizada, permiten sugerir la implementación de la propuesta del sistema de gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información), en las medianas empresas ferreteras de la ciudad de Guatemala, para integrar la gestión de riesgos a la toma de decisiones.

2. Luego de realizada la implementación de la propuesta de gestión de riesgo de activos informáticos, es necesario que se haga el seguimiento correcto para verificar que el modelo de recolección de datos, las matrices de riesgo de procesos y la ponderación de riesgos se realice adecuadamente, para que los resultados sean favorables en la identificación de procesos de negocio en los que el riesgo de activos informáticos sea crítico.

3. Para que el personal se identifique con la propuesta, se propone realizar actividades adicionales que promuevan la cultura de gestión de riesgo de activos informáticos en las empresas medianas del sector ferretero de la ciudad de Guatemala.

4. Se sugiere la inclusión del modelo de gestión de riesgos de activos informáticos como parte de los planes estratégicos de las empresas, para apoyar el alcance de sus objetivos financieros.

5. Se debe definir un responsable en la organización como principal impulsor y generador de la gestión de riesgo de activos informáticos para dar sustentabilidad a largo plazo de los beneficios del sistema de gestión propuesto.

6. Llevar a cabo monitoreo proactivo de niveles de exposición al riesgo de activos informáticos en los procesos prioritarios de las empresas, para la

aplicación integral del marco de trabajo RISK IT (Riesgo de Tecnología de la Información),

7. Evaluar otros sectores de industria de medianas empresas en la ciudad de Guatemala, que se puedan beneficiar del sistema de gestión de gestión de riesgo de activos informáticos a través del marco de trabajo RISK IT (Riesgo de Tecnología de la Información).

BIBLIOGRAFÍA

Libros

1. Cohen Karen, D. y Asín Lares, E. (2009). Tecnologías de información en los negocios. México. McGraw Hill. Quinta edición.

2. Fields, Edward. 2016. Finanzas esenciales para gerentes no financieros y contables, Tercera Edición. Capitulo tres, estados de flujo de caja. 365 p. Editorial AMACOM.

3. Gallegos, M. A. (2015). Integrando el riesgo de TI con el riesgo operacional. Calves para su implementación exitosa.

4. Gilbert, S. D. 2016. Daños económicos y responsabilidad legal en los negocios. Capítulo 2, pérdida económica. 150 p. Editorial Business Expert Press.

5. González López, M. A. (2017). El auditor externo en la evaluación de empresa en funcionamiento según Norma Internacional de Auditoría 5701, aplicada a una ferretería. Licenciatura en Contaduría Pública y Auditoría. Facultad de Ciencias Económicas. Usac.

6. Guitert Catasús, M. y Barajas Frutos, M. (2004). Las tecnologías de la información y comunicación. España.

7. Hernández Sampieri, R.; Fernández Collado, C.; y, Baptista Lucio, P. (2014). Metodología de la Investigación. México. Sexta Edición. McGraw-Hill Interamericana.

8. IICA/CATIE. Instituto Interamericano de Cooperación para la Agricultura. (1999). Redacción de Referenciar Bibliográficas: Normas Técnicas del IICA Y CATIE. Turrialba, Costa Rica. Biblioteca Conmemorativa Orton. Cuarta edición.

9. INCIBE. Instituto Nacional de Ciberseguridad. (2017). Gestión de riesgos. Una guía de aproximación para el empresario. España.

10. ISACA. (2007). Valor para la empresa: Buen Gobierno de las Inversiones en TI. El Caso de Negocio.

11. ISACA. (2009). Marco de riesgos de TI. Risk IT basado en COBIT.

12. ISACA. (2012). Programa de Aseguramiento de enfoque de auditoría y gestión de riesgos de TI. Resumen ejecutivo.

13. ISO 27001. (2008). Information Classification Policy

14. Kogan, Paul Hopkins 2017. Fundamentos de gestión de riesgo: Entendiendo, evaluando e implementando gestión de riesgo efectiva. Gestión de riesgo empresarial, capítulo 8. Definiciones de ERM. 488 p. Editorial Kogan Page Limited.

15. Lizarraga, J. (2005). ISO 27001: El estándar de seguridad de la información.

16. Parrino, Robert; Kidwell, David S. 2009. Fundamentos de finanzas corporativas. Proyecciones y planificación financiera, capítulo 19. Editorial John Wiley and Sons.

17. PMI. (2013). La guía del cuerpo de conocimientos de la gestión de proyectos. Gestión de integración de proyectos, capítulo 4. 616 p. Quinta edición, instituto de gestión de proyectos.

18. Romero Mora, P.; Saldívar Vaquera, C. E.; Delgado Ibarra, R.; y, Sánchez Montúfar. (2014). México. Pearson educación. Primera edición.

19. Treviño Gelover, E. (2009). Riesgo empresarial: identificación, gobierno y administración del riesgo de TI. España.

20. Van Horne, C. J. y Wachowicz, J. M. (2010). Fundamentos de administración financiera. México. Pearson educación. Decimotercera edición.

Normativa

1. Universidad de San Carlos de Guatemala. Facultad de Ciencias Económicas. Escuela de Estudios de Postgrado. (2009). Guía metodológica para la elaboración del plan e informe de investigación de postgrado de Ciencias Económicas.

2. Universidad de San Carlos de Guatemala. Facultad de Ciencias Económicas. Escuela de Estudios de Postgrado. (2009). Normativo de Tesis para optar al grado de Maestro en Ciencias.

Consultas en Línea

1. ¿Qué es el riesgo?, (2004). Consultado el 15 de Febrero de 2017. Recuperado de: https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf, UNISDR.

2. Acuerdo Gubernativo 211 (2015), clasificación de las pequeñas, micro y medianas empresas. Consultado el 17 de febrero 2017. Recuperado de: http://www.mineco.gob.gt/sites/default/files/ag_211-2015.pdf

3. El estándar de gestión de riesgos (2012), definición de gestión de riesgo. Consultado el 15 de febrero del 2017. Recuperado de: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

4. DCA. Diario de Centro América. (2012). Ferreterías de la Cuarta Avenida (2012). Consultado el 15 de noviembre de 2016. Recuperado de: https: //dca.gob.gt/noticias-guatemala-diario-centro-america/category/editoriales/

5. Historia de la ferretería el globo (2016), consultado el 15 de noviembre de 2016. Recuperado de: http://www.ferreteriaelglobo.com/sobre.php

6. Historia de la ferretería La Llave (2016), consultado el 15 de noviembre de 2016. Recuperado de: http://www.lallave.com.gt/

7. Historia de la ferretería Lewonski (2016), consultado el 15 de noviembre de 2016. Recuperado de: http://www.lewonski.com/index.php/?page_id=2

8. Marco de trabajo RISK IT, (2009). Consultado el 15 de Noviembre de 2016. ISACA. Recuperado de: https://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Spa_0610.pdf

9. VAL IT (2017), consultado el 11 de febrero de 2017. Recuperado de: http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx

ANEXOS

Anexo 1
Encuesta Inicial

1. ¿Es la empresa una ferretería?

- ◯ Si
- ◯ No

2. ¿Es la empresa considerada mediana empresa? (81-200 trabajadores, con ventas anuales entre 9 y 40 millones de Quetazles?

- ◯ Si
- ◯ No

3. ¿Se utiliza en la empresa algún tipo de tecnología para llevar a cabo los negocios? Por ejemplo: Software, Hardware, etc.

- ◯ Si
- ◯ No

4. Si la respuesta anterior fue afirmativa, por favor seleccione las opciones disponibles para representar que tipo de componentes tecnológicos existen en la operación de la empresa:

- [ ] Computadoras
- [ ] Smartphones
- [ ] Sitios Web / Internet
- [ ] Software variado como office, sistemas de gestión de procesos, etc.
- [ ] Dispositivos de seguridad de redes como firewalls
- [ ] Antivirus
- [ ] Correo electrónico
- [ ] Impresoras
- [ ] Redes inalámbricas
- [ ] Carpetas compartidas por la red
- [ ] Proyectores
- [ ] Routers
- [ ] Servidores
- [ ] Otro (Cualquier otro dispositivo no listado). Si desea puede agregar comentarios.

5. En los procesos de negocio mencionados, ¿Que nivel de participación hay por parte de los componentes tecnológicos de la empresa? Indique la escala, siendo 1 la menor y 5 la mayor utilización.

No se utiliza tecnología en los procesos de negocio	La tecnología se utiliza poco en el 25% de los procesos de negocio	La tecnología se utiliza habitualmente en el 50% de los procesos	La tecnología se utiliza frecuentemente y en el 75% de los procesos	La tecnología se utiliza frecuentemente y en 100% de los procesos de negocio
☆	☆	☆	☆	☆

6. ¿Cuales procesos de negocio que existen en la empresa? (Nombre genérico de proceso)

- [ ] Ventas
- [ ] Mercadeo
- [ ] Inventario
- [ ] Facturación
- [ ] Nómina
- [ ] Contratación
- [ ] Gestión Interna de recurso humano
- [ ] Entrenamiento
- [ ] Contabilidad
- [ ] Tecnología de la Información
- [ ] Servicio al cliente
- [ ] Planificación estrátegica
- [ ] Planificación financiera
- [ ] Otro (especifique)

Anexo 2

Cuestionario adicional para conocer la escala de impacto financiero

Cuestionario Adicional				
¿Cómo cataloga usted que los impactos financieros afectan a la empresa? Considere la siguiente escala: No significativo, bajo, medio, alto y crítico. Por favor indique el rango de valores anuales para cada categoría como se muestra en el ejemplo.	Ejemplo limite Inferior	Ejemplo limite superior	Ingrese su límite inferior	Ingrese su límite superior
No Significativo	-	10,000		
Bajo	10,000	20,000		
Medio	20,000	30,000		
Alto	30,000	40,000		
Crítico	40,000	Más de 50,000		

Considere:	Definición
No Significativo	No tiene consecuencias relevantes a las finanzas de la empresa.
Bajo	Tiene consecuencias mínimas y plantea recuperación de valor en corto plazo con esfuerzo mínimo por parte de la empresa.
Medio	Tiene consecuencias considerables y plantea recuperación de valor en mediano plazo con esfuerzo medio por parte de la empresa. Puede poner o no en riesgo la salud financiera de la organización.
Alto	Plantea consecuencias financieras severas y con recuperación de valor a largo plazo. Se considera el tipo de riesgo que potencialmente dificultaría alcanzar los resultados reduciendo considerablemente el potencial de generación de rentabilidad.
Crítico	Impacto severo que atenta con la vida misma de la empresa y que tiene como consecuencias la no rentabilidad de los ejercicios operativos. La recuperación de este tipo de impactos es incierta.

Anexo 4
Cuestionario entrevista a gestores de riesgo y gestores de TI

No.	Pregunta	Respuestas/Anotaciones:
1	¿Cual es su rol en la organización?	
2	¿Gestiona usted riesgos de TI de la empresa?	
3	¿Participa usted en la gestión de incidentes de TI que repercuten en interrupciones de operaciones de procesos de negocio?	
4	¿Tienen datos estadísticos de la cantidad de incidencias de TI y de la duración de las incidencias?	
5	¿Es posible identificar por activo informático la recurrencia de fallas?	
6	¿Es posible identificar por activo informático los procesos afectados a causa de las fallas de TI?	
7	¿Existe posibilidad de compartir los resumenes de datos estadísticos de la gestión de incidencias de la organización para ser utilizados en el desarrollo de la investigación?	

Anexo 5
Cotización Servidores primario y Secundario

PowerEdge R640

Ideal balance of density and scalability

Get scalable computing and storage in a 1U, 2-socket platform with an ideal mix of performance, cost and density for most data centers.

Starting at $3,646.24

View configurations

PowerEdge R530 Rack Server

Built for versatility.

Deliver balanced performance and midrange scalability with a powerful 2S/2U rack server.

Starting at $1,509.00

View configurations

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES