UNIVERSIDAD ANDINA SIMON BOLIVAR

SEDE ECUADOR

ÁREA DE GESTIÓN

PROGRAMA DE MAESTRIA EN FINANZAS

Y GESTION DE RIESGOS

"ADAPTACION DE UN MARCO METODOLOGICO PARA LA MEDICION DEL RIESGO OPERATIVO GENERADO POR PUNTOS VULNERABLES DE TECNOLOGÍAS DE INFORMACION CON UN ENFOQUE DE AUDITORIA BASADO EN RIESGOS EN EL ECUADOR"

Andrés Gustavo Aguayo Yépez

2011

Al presentar esta tesis como uno de los requisitos previos para la obtención del título de "Magíster en Finanzas y Gestión de Riesgos", autorizo al Centro de Información de la Universidad para que haga de este trabajo un documento disponible para su lectura según las normas de la institución.

También cedo a la Universidad Andina Simón Bolívar, los derechos de publicación de este trabajo o de partes de ella, manteniendo mis derechos de autor hasta por un período de 30 meses contados después de su aprobación.

Andrés Gustavo Aguayo Yépez
TEC. ESP. FIN. ING. COM. CPA.

Quito, diciembre de 2011

UNIVERSIDAD ANDINA SIMON BOLIVAR

SEDE ECUADOR

ÁREA DE GESTIÓN

PROGRAMA DE MAESTRIA EN FINANZAS

Y GESTION DE RIESGOS

"ADAPTACION DE UN MARCO METODOLOGICO PARA LA MEDICION DEL RIESGO OPERATIVO GENERADO POR PUNTOS VULNERABLES DE TECNOLOGÍAS DE INFORMACION CON UN ENFOQUE DE AUDITORIA BASADO EN RIESGOS EN EL ECUADOR"

Andrés Gustavo Aguayo Yépez

Director: Econ. Iván Velástegui

Quito, diciembre de 2011

"ADAPTACION DE UN MARCO METODOLOGICO PARA LA MEDICION DEL RIESGO OPERATIVO GENERADO POR PUNTOS VULNERABLES DE TECNOLOGÍAS DE INFORMACION CON UN ENFOQUE DE AUDITORIA BASADO EN RIESGOS EN EL ECUADOR"

RESUMEN

A lo largo de los últimos años se ha tomado conciencia de la importancia que reviste la gestión de riesgos para un gobierno corporativo fuerte. Las organizaciones se sienten bajo presión y deben identificar todos los riesgos de negocio que enfrentan: sociales, éticos, ambientales, financieros y operativos; además de explicar cómo los gestionan para lograr un nivel aceptable. Mientras tanto, se ha extendido el uso de los enfoques de gestión de riesgos para todas las empresas a medida que las organizaciones reconocen sus ventajas.

Las personas llevan a cabo actividades de gestión de riesgos para identificar, evaluar, gestionar y controlar todo tipo de eventos o situaciones. Estos pueden variar abarcando desde tipos de riesgo para proyectos únicos o estrictamente definidos, como por ejemplo: los riesgos de mercado, hasta amenazas y oportunidades que debe afrontar la organización como una sola unidad.

La naturaleza del negocio bancario como tal, lleva implícita la misión y el deber de administrar adecuadamente el riesgo. Las crisis financieras ocurridas en varios países, incluido el Ecuador, pusieron en evidencia la importancia de saber manejar los riesgos asociados a este sector y a estar alertas ante la fragilidad de los sistemas de medición y control de riesgos.

Este estudio tiene como finalidad convertirse en un aporte cualitativo y técnico sobre las debilidades detectadas a través de la identificación de puntos vulnerables en las tecnologías de información y aquellas que hacen referencia específicamente a la gestión tecnológica como tal, que incrementa actualmente el riesgo operativo en las instituciones financieras, utilizando como guía de trabajo un enfoque de riesgos conforme lo requiere la norma, la legislación ecuatoriana y las mejores prácticas establecidas por el Comité de Basilea.

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño…

A mis padres: Elizabeth Yépez Cabezas y Raúl Aguayo Berrones, por enseñarme el amor al estudio, ustedes me dieron la vida y han estado conmigo en todo momento, gracias por darme una carrera para mi futuro y por creer en mí los amo, gracias a ustedes he llegado a esta meta…

A mi hermano: Daniel Aguayo Yépez por estar ahí inspirando mi vida te dedico mi tesis con todo mi corazón, siempre estaré junto a ti…

Mammy your arms are always open when I need a hug. Your heart knows you understand when I need a friend. Your sensitive eyes harden when I need a lesson. Your strength and love I have gone through life and given me wings to fly when I was in need love you madly thanks to exist…

AGRADECIMIENTO

A ti DIOS que me diste la oportunidad de vivir y de regalarme una familia maravillosa, sin ti en mi vida nada tendría sentido, permíteme ser capaz de iluminar la vida de mis seres queridos…

A ustedes Papá y Mamá por enseñarme a luchar hacia delante, por su gran corazón y capacidad de entrega, pero por sobretodo por enseñarme a ser responsable…

A mi Universidad Andina Simón Bolívar, por darme la oportunidad de aprender y forjarme como profesional…

A mi tutor: Iván Velástegui, por su paciencia y dedicación para la realización de esta tesis…

INDICE GENERAL

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

CAPÍTULO II
METODOLOGIA DE LA INVESTIGACIÒN

CAPÍTULO III

POR QUÈ UN ENFOQUE DE AUDITORÌA BASADO EN RIESGOS?

CAPÍTULO IV

GESTIÓN DE RIESGOS CORPORATIVOS MARCO INTEGRADO “COSO IRM” Y PRINCIPIOS FUNDAMENTALES GREC

CAPÍTULO V

EL RIESGO OPERATIVO Y LOS PUNTOS VULNERABLES EN LAS TECNOLOGIAS DE INFORMACIÓN

CAPÍTULO VI

CASO DE APLICACIÓN: MODELACIÓN DE LA ADAPTACIÓN METODOLÓGICA

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

El sistema bancario y financiero es uno de los sectores importantes de la economía de un país y en los últimos años ha evolucionado notablemente, existen cambios e innovaciones importantes, tanto en la operativa misma del sector, el mercado de valores, la complejidad del comercio exterior, así como en la automatización de los sistemas, cuya magnitud y resultados han sido beneficiosos para el sector bancario. Igual impacto se ha observado en el movimiento de capitales a través de este sector.

Este crecimiento determina también una exposición a riesgos cada vez mayores, producto del aumento de la volatilidad en los flujos de capital, en las tasas de interés, y en una mayor utilización de productos financieros estructurados a la medida de los clientes, en función a sus preferencias de riesgo y necesidades, la velocidad de la innovación tecnológica con la que actualmente se realizan las operaciones, así

como la velocidad de la transferencia de información necesaria para cada una de las actividades referidas.

En los últimos años se ha tomado conciencia de la importancia de efectuar una eficiente y efectiva gestión de riesgos para un gobierno corporativo, existen organizaciones que se encuentran bajo presión y requieren identificar todos los riesgos asociados a sus negocios, esto ha derivado en que las organizaciones cada vez desarrollen enfoques de riesgo en la medida en que observan sus ventajas[1]. La naturaleza del negocio bancario como tal, lleva implícita la misión y el deber de administrar adecuadamente el riesgo. Las crisis financieras ocurridas en varios países, incluido el Ecuador, pusieron en evidencia la importancia de saber manejar los riesgos asociados a este sector y a estar alertas ante la fragilidad de los sistemas de medición y control de riesgos.

Con estos antecedentes, las instituciones financieras del país enfrentan la necesidad de identificar, medir y controlar con precisión, los niveles de riesgos asumidos. Paralelamente, los organismos de control bancario han reorientado su trabajo hacia la supervisión preventiva de riesgos. Ambas situaciones, revelan la creciente importancia que la gestión de riesgos ha cobrado en los últimos años en los que el Sistema Financiero Nacional e Internacional ha tenido un crecimiento muy importante, tanto en flujos de capital como en la diversidad de productos que se han

[1] The Institute of Internal Auditors (2004). El rol de la auditoría interna en relación con la gestión de riesgos para toda la empresa (paper).

incorporado al mercado, a consecuencia de la innovación financiera y tecnológica.

Este estudio tiene como finalidad convertirse en un aporte cualitativo y técnico sobre las debilidades detectadas a través de la identificación de puntos vulnerables en las tecnologías de información y aquellas que hacen referencia específicamente a la gestión tecnológica como tal, que incrementa actualmente el riesgo operativo en las instituciones financieras, utilizando como guía de trabajo un enfoque de riesgos conforme lo requiere la norma, la legislación ecuatoriana y las mejores prácticas establecidas por el Comité de Basilea.

1.1. OBJETIVO GENERAL.

Contar con un instructivo enmarcado en el marco metodológico: Committee of Sponsoring Organizations (COSO) – Enterprise Risk Management (ERM), Control Objectives for Information and Related Technology (COBIT) y Manual de Supervisión y Calificación de la Superintendencia de Bancos y Seguros del Ecuador (GREC), para medir el riesgo operativo en los procesos de gestión tecnológica utilizando una matriz de riesgo operativo basado en factores de riesgo.

1.2. OBJETIVOS ESPECIFICOS.

La sistematización y la posterior aplicación de las mejores prácticas de gestión de riesgos, permite apoyar a las Instituciones del Sistema Financiero Nacional objeto del estudio, a través de los siguientes objetivos específicos:

- Investigar, analizar y determinar el nivel de riesgo que tienen los siguientes procesos de gestión tecnológica: administración de infraestructura, desarrollo mantenimiento e implementación de software, gestión de seguridad de información, gestión de soporte a usuarios, monitoreo de sistemas y aplicaciones, y procesamiento tecnológico.

- Construir la matriz de riesgo operativo de los procesos antes detallados usando factores de riesgo y además aplicando los criterios de evaluación cualitativo y cuantitativo.

1.3. HIPOTESIS.

La presente investigación plantea una hipótesis a ser comprobada, orientada a verificar que: “la adaptación de un marco metodológico para la medición del riesgo operativo generado por puntos vulnerables de tecnologías de información con un enfoque de auditoría basado en riesgos , derivan en una Aplicación Efectiva de las Mejores Prácticas de Gestión para un Modelo de Riesgos”

CAPITULO II

METODOLOGIA DE LA INVESTIGACIÓN

2.1. ENFOQUE TEÓRICO.

Para el desarrollo del presente estudio, se realizó una fundamentación teórica basada en las siguientes metodologías ampliamente conocidas y que ostentan ser aquellas que dominan las mejores prácticas en materia de riesgos.

Metodología COSO (Committee of Sponsoring Organizations)

Es el marco metodológico de referencia que contribuye con la identificación y coordinación de todos los elementos que deben ser considerados para el ejercicio de una efectiva gestión del riesgo dentro de la organización, buscando disminuir la posibilidad de incurrir en pérdidas a razón de su operación dado el normal giro del negocio.

Este marco conceptual esta desarrollado con un enfoque de administración de riesgo integral y empresarial que incluye: el planteamiento, la formulación y el seguimiento de un proceso básico de identificación, evaluación, medición, reporte de amenazas, debilidades, fortalezas y oportunidades que afectan el logro de las metas y objetivos de la organización, para en base a ellos ser medidos en términos monetarios para ser administrados en función de las expectativas y del apetito al riesgo que haya establecido la organización.

Metodología COBIT (Control Objectives for Information and Related Technology)

Es el marco de referencia que facilita y permite la estructura de relaciones y procesos para dirigir y controlar a la organización con la finalidad de alcanzar sus objetivos mediante la generación de valor a través de las tecnologías de la información.

La metodología COBIT se aplica a los sistemas de información de toda la organización incluye: las computadoras personales, mini computadoras, y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para alcanzar sus objetivos.

Metodología GREC (Manual de Supervisión y Calificación de la Superintendencia de Bancos y Seguros del Ecuador)

Esta metodología hace énfasis en aspectos cualitativos, enfocándose en el gobierno corporativo y en la gestión de riesgos como tal, su aplicación a través de modelos de administración de riesgos proveen un esquema con estructura genérica formal, ordenada, integral y lógica para desarrollar un enfoque adecuado de gestión, recoge además las mejores prácticas internacionales observando la realidad ecuatoriana, abordando un proceso de supervisión orientado a riesgos.

2.2. ENFOQUE METODOLÒGICO DE ESTUDIO.

La investigación por su origen propio de datos es documental y de campo dado que en primera instancia se consultó todo tipo de documentos que han dejado (y/o dejan) constancia material a través del tiempo sobre el tema a desarrollar. Posteriormente se realizó el levantamiento de información en una serie de instituciones financieras del medio local, a través de observación, interrogatorios, experimentación y constatación física.

La investigación por su profundidad es descriptiva y explicativa, dado que se realiza buscando conocer las características del estudio para ser estudiado a un nivel de detalle relevante, así como tratar de encontrar una relación de causa y efecto entre las variables inmersas en el mismo.

Esta investigación no experimental es de tipo longitudinal, en función de que se recolectó información en distintos momentos temporales, particularmente sobre eventos relacionados datos y registros de procesos relevantes que hayan sucedido en el pasado inmediato, no se utilizó métodos ni modelos estadísticos en este estudio dado que la data de información es limitada.

La investigación por su originalidad es primaria, dado que el proyecto de investigación se basa en el objeto de estudio.

2.3. PROCESAMIENTO DE LA INFORMACIÓN.

Para realizar la presente investigación se procedió a realizar:

- Revisión documental de las buenas prácticas emanadas del Comité de Basilea en lo referente a la gestión del riesgo operativo.

- Homologar los procesos más importantes de gestión tecnológica en las instituciones financieras del país.

- Adaptación metodológica para una adecuada gestión de riesgos operativos en los procesos de interés.

- Adecuación de herramientas de levantamiento de información.

- Levantamiento y relevamiento de información de los procesos de gestión tecnológica (administración de infraestructura, desarrollo mantenimiento e implementación de software, gestión de seguridad de información, gestión de soporte a usuarios, monitoreo de sistemas y aplicaciones, y procesamiento tecnológico) donde se evidencia la existencia de componente tecnológico.

- Aplicación de planes de acción acorde a la guía de las mejores prácticas.

- Validación de hipótesis.

- Presentación de resultados obtenidos.

CAPITULO III

POR QUÉ UN ENFOQUE DE AUDITORIA BASADO EN RIESGOS?

3.1. UNA NECESIDAD DE NEGOCIO Y UN REQUERIMIENTO REGULATORIO ACORDE A LAS MEJORES PRÁCTICAS INTERNACIONALES.

"Los mercados de capital en los países de América Latina y en particular en los países andinos se caracterizan por un escaso nivel de desarrollo relativo que se refleja en una baja profundización financiera e incipiente capitalización bursátil. Esta situación limita las oportunidades de acceso a mayores y más eficientes fuentes de financiamiento para la producción e inversión del sector empresarial, constituyéndose en un importante obstáculo para incrementar la competitividad en la región[2]".

Esta debilidad financiera de la región y tomando en cuenta que las organizaciones se desenvuelven en diversos ambientes en los que se realizan actividades de auditoría interna, afectan la práctica de la

[2] García, Enrique (2005). Lineamientos para un Código Andino de Gobierno Corporativo. Eficiencia, equidad y transparencia en el manejo empresarial (Revisión Marzo 2006, Corporación Andina de Fomento, (paper).

auditoria como tal, y hacen cada vez más necesario incorporar un amplio marco de normas que faciliten establecer principios básicos para la práctica y el ejercicio de la auditoría interna que promueva actividades que generen valor agregado, que faciliten la medición del desempeño de una auditoría interna integral, y que por supuesto a través del desarrollo de su trabajo ayude a mejorar las operaciones y los procesos de la organización.

El desarrollo de este nuevo enfoque de Auditoría Interna requirió, a su vez una actualización de la definición del concepto de la auditoría interna[3], la cual fue emitida por el Instituto de Auditores Internos en el mes de junio de 1999, que señala:

"La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, cuya finalidad es aumentar el valor y mejorar las operaciones de la organización. Ayuda a que la organización cumpla con sus objetivos mediante la aplicación de un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de manejo de riesgos, control y dirección"

Esta nueva manera de concebir la auditoria hace hincapié en las prácticas denominadas en inglés "The Best Practices", recomendadas

[3] La antigua definición que data desde el 1946 del Instituto de Auditores Internos IAI, indica: "La auditoría interna es una función independiente de control, establecida como un servicio dentro de una organización para examinar y evaluar sus actividades. El objetivo de la auditoría interna es ayudar a los miembros de la organización en el cumplimiento efectivo de sus responsabilidades. A este fin, les proporciona análisis, valoraciones, recomendaciones, consejo e información, relativos a las actividades revisadas"

por Instituto de Auditores Internos, en donde se establece: a) debe contribuir a la identificación de riesgos de negocio; b) debe tomar un rol de liderazgo cuando se habla de riesgo en la organización; c) debe cambiar la mentalidad de evaluar controles a evaluar riesgos de negocio; d) los servicios que se brindan a razón de la auditoria deben agregar valor en todo momento a la organización.

3.2. NORMAS INTERNACIONALES DE AUDITORIA INTERNA Y LEGISLACION LOCAL, SU IMPORTANCIA Y SU RELACION CON EL RIESGO OPERATIVO.

La Auditoría Interna hasta hace poco fue considerada a nivel mundial como una actividad de evaluación dentro de las organizaciones, para examinar, evaluar y monitorear de manera adecuada eficiente y eficaz el sistema de control interno-contable, también se le han asignado funciones para determinar la eficacia y eficiencia económica de los sistemas operacionales y los controles gerenciales encaminados a verificar la razonabilidad de las entradas y salidas de recursos financieros.

A partir de la década de los ochenta y noventa, y a partir de los cambios tecnológicos surgidos en la automatización de las transacciones en línea y tiempo real, las nuevas teorías de gestión en la administración y el control, la globalización de la economía, es evidente que el ambiente en el manejo de los negocios sufrió cambios importantes que afectaron

indudablemente la auditoría interna a nivel internacional y mundial, es por ello que hoy en día los auditores internos están obligados a tener conocimientos suficientes de los riesgos y controles clave que existen en las tecnologías de la información y de las técnicas de auditoría disponibles basadas en tecnología que le permitan desempeñar el trabajo asignado de manera efectiva. El auditor interno debe ejercer el debido cuidado profesional al considerar[4]:

- La determinación del alcance es necesario para lograr los objetivos del trabajo con relación a los procesos que se auditan así como a los resultados a los que pretende llegar;

- El impacto, la magnitud y cuantía económica en asuntos a los cuales se aplican procedimientos de aseguramiento (auditoria);

- La adecuación y eficacia de los procesos de gobierno, gestión de riesgos y control;

- La probabilidad de obtención de errores significativos, fraude o incumplimientos; y,

- El costo de aseguramiento en relación con los beneficios potenciales.

[4] Consejo Para la Práctica 1220-1: Debido cuidado profesional - THE INSTITUTE OF INTERNAL AUDITORS.

3.3. NORMAS PARA EL EJERCICIO PROFESIONAL DE LA AUDITORIA INTERNA EN EL SISTEMA FINANCIERO ECUATORIANO.

En la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, se define a la unidad de auditoría interna en los siguientes términos: “La auditoría interna es una actividad de asesoría, independiente y objetiva, diseñada para agregar valor y asegurar la corrección de las operaciones de una institución. Ayuda al cumplimiento de los objetivos de una organización, brindando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de la administración del riesgo, el control y los procesos organizacionales presentes y futuros. El 21 de enero de 2010, la Junta Bancaria emitió la resolución No. JB-2010-1549, señalando textualmente lo siguiente:

"Incluir como artículo No. 20, el siguiente y renumerar el restante: “ARTÍCULO 20.- En lo que no se oponga a lo previsto en la normatividad de la Superintendencia de Bancos y Seguros, serán de aplicación las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, así como el Código de Ética emitidos por The Institute of Internal Auditors (IIA). En el caso de los auditores de sistemas, se tomarán en consideración las directrices de auditoría previstas por el Information Systems Audit and Control Association (ISACA)”"

Las normas internacionales para el ejercicio profesional de la auditoría interna contienen 42 consejos para la práctica, adicionalmente existen 2 declaraciones denominadas “de posición” que hablan del rol de la auditoría interna en relación con la gestión de riesgos y las alternativas de obtención de recursos para el cumplimiento de la función de auditoría interna.

Las normas referidas en el párrafo antecedente se actualizaron en octubre del año 2008 y entraron en vigencia el 1ro de enero de 2009 a nivel mundial.

3.4. EL ROL DEL AUDITOR INTERNO FRENTE AL CONTROL INTERNO Y A LA GESTION DE RIESGOS.

El rol del auditor interno y el ejercicio de la auditoría interna ha cambiado indudablemente ya que los esfuerzos, los recursos y la atención de los reguladores (entes de control) se desvió del análisis de la operación del negocio como tal para orientarse en:

- Determinar tipos de riesgos a los que se exponen las organizaciones independientemente de la industria a la cual pertenezcan, evaluando el impacto y la magnitud del riesgo en ellas.

- Evaluar y valorar los mecanismos utilizados en la organización para manejar, administrar y controlar sus exposiciones de riesgo, y;

- Evaluar si la administración y/o la alta gerencia (directores) monitorean de manera activa y permanente la exposición de sus organizaciones a los riesgos asociados a sus industrias. (benchmarking).

Por lo mencionado, la auditoría interna ha tenido que cambiar algunos paradigmas sobre los cuales se sustentaba el enfoque, el rumbo, y la ejecución de la auditoría como tal hasta hace unos pocos años, siendo uno de los principales cambios el de modificar el enfoque basado en controles por el enfoque de auditoría basada en riesgos, y pasar de emitir reportes de hechos pasados por procurar desarrollar actividades proactivas.

La aplicación de este enfoque de evaluación de riesgos permite orientar los recursos y las revisiones hacia las áreas de la organización que generan más valor, canaliza un mejoramiento constante a través del conocimiento del negocio y la organización como tal, y finalmente incorpora la tecnología de la información con la utilización de equipos y softwares especiales que incrementan la productividad de las actividades, al automatizar las rutinas de trabajo para acceder a las

distintas bases de datos y para presentar y difundir los hallazgos de auditoría.

En el siguiente esquema detallado en el libro de *Risk Management: Changing the internal Auditor´s Paradigm,* de David McNamee, se detallan los cambios en los paradigmas que han modificado el alcance de la auditoría interna:

Cuadro No. 1.

CARACTERISTICAS	ANTIGUO PARADIGMA	NUEVO PARADIGMA
Enfoque de la AI.	Control Interno.	Riesgos del negocio.
Respuesta.	Reactiva, posterior a los hechos. Observadores de las iniciativas del plan estratégico.	Proactiva, en tiempo real. Monitoreo continuo y participación en el proceso del plan estratégico.
Pruebas de AI.	Importancia de los controles.	Importancia de los riesgos.
Métodos de AI.	Énfasis en integridad de la evaluación de controles detallados.	Énfasis en la importancia de una cobertura de los riesgos del negocio.
Recomendaciones de AI.	Controles Internos: -Fortalezas / debilidades. - Costo / beneficio. -Eficiencia / Efectividad.	Manejo del Riesgo: -Evitarlos / diversificarlos -Repartirlo / transferencia -Controlarlos / aceptarlos
Informes de AI.	Dirigidos hacia la funcionalidad de controles.	Dirigidos hacia el proceso de riesgos.
Rol de la AI en la organización.	Función de evaluación independiente de los controles internos.	Integración en el manejo del riesgo y comunicación continua con la Dirección

CAPITULO IV

GESTION DE RIESGOS CORPORATIVOS MARCO INTEGRADO "COSO IRM" Y PRINCIPIOS FUNDAMENTALES GREC

4.1. LA METODOLOGIA COSO – IRM, IMPORTANCIA Y BASES METODOLÓGICAS.

El modelo de control denominado COSO "Control Interno – Marco Integrado" fue desarrollado con la participación de algunas organizaciones profesionales de contadores, de ejecutivos en finanzas y de auditores internos, con la finalidad de ir hacia un mejoramiento continuo y permanente del control interno y un mejor gobierno corporativo. Por supuesto la generación de esta metodología fue una iniciativa del sector privado en donde se unieron cinco organizaciones para formar COSO:

- American Institute of Certified Public Accountants.
- American Accounting Association.
- Financial Executives Institute.

- The Institute of Internal Auditors.
- Institute of Management Accountants.

El objetivo fundamental de la aplicación de COSO es impulsar una cultura administrativa en todo tipo de organizaciones sugiriendo el desarrollo un plan a la organización que procure la salvaguarda de sus activos, la exactitud y la confiabilidad de la información financiera y contable, el promover en todo tiempo la eficiencia operacional y fomentar el apego a las políticas y procedimientos internos.

La misión de COSO fue mejorar la calidad de la información financiera mediante un enfoque en el gobierno corporativo, los controles internos y las normas éticas, dos metas principales se establecieron:

- Establecer una definición común y universal de control interno.

- Promover una norma a partir de la cual las organizaciones sin importar a que sector pertenezcan puedan evaluar sus controles internos.

En el marco metodológico de COSO hace hincapié en que el sistema de control interno, es un mecanismo y una herramienta pero que no sustituye a la gerencia y que los controles deben incorporarse y no agregarse a actividades operativas.

De igual manera aborda limitaciones de un sistema de control interno y claro los roles y responsabilidades de las partes que afectan al sistema, se incluyen en estas limitaciones el juicio de opinión incorrecto, las instrucciones mal entendidas, errores en general, hacer caso omiso a la gerencia, la colusión y la no consideración de costo/beneficio. Se pretende superar estas limitaciones aplicando COSO integralmente pretendiendo tener un grado de seguridad razonable en cuanto a la consecución de objetivos organizacionales.

Cuadro No. 2.

Directores:	Establece objetivos y supervisa la administración de riesgos. Define el apetito al riesgo. Visión del portafolio de riesgos. Rapidez de respuesta al riesgo.
Gerencia General-CEO:	Proporciona liderazgo y orientación a la alta dirección y establece políticas amplias que reflejen la administración de riesgos de la entidad así como su riesgo aceptado.
Gerentes División:	Los responsables de las unidades de negocio, procesos de negocio y departamentos funcionales de las distintas líneas son quienes deben identificar, evaluar y responder al riesgo en relación con el logro de sus objetivos y el cumplimiento de las políticas de administración de riesgos de la entidad.
	Asignar a los gerentes de sus unidades, las responsabilidades específicas en la administración de riesgos corporativos.
Comité de Administración de Riesgos Corporativos:	Responsabilidad global del proceso de administración de riesgos corporativos, incluyendo los procesos utilizados para identificar, evaluar, responder informar sobre el riesgo. Definición de roles y responsabilidades de rendir cuentas ante la alta dirección, dotación de políticas, marcos, metodologías y herramientas a las unidades de negocio para la identificación, evaluación y administración de riesgos. Revisión del perfil de riesgo de la entidad.

Oficial de Riesgo:	Trabaja con otros directivos para establecer una administración efectiva de riesgos corporativos en sus respectivas áreas de responsabilidad.
Auditoría Interna:	Monitoreo de la implantación de la administración de riesgos corporativos: tanto en su diseño como en sus funciones. Evalúa las mejoras en la administración de riesgos.
	Requerimientos especiales de la Gerencia.
	Efectividad y eficiencia de la respuesta al riesgo y de las actividades de control implementadas.
	Completitud y exactitud de los reportes sobre la administración de riesgos corporativos.
	Participar en Directorio - Comité de Auditoría - Otros Comités

De igual manera establece los siguientes elementos de la administración de riesgos corporativos:

Cuadro No. 3.

ELEMENTOS DE LA ADMINISTRACION DE RIESGOS CORORATIVOS	SUB-ELEMENTOS	RELACION CON LAS INSTITUCIONES FINANCIERAS
Ambiente de Control:	Filosofía de la administración del riesgo.	Declaración de la administración con referencia a su filosofía de administración de riesgos. Prudencia versus riesgo. Formalidad versus informalidad.
	Cultura de riesgos.	Por lo general se evalúa con encuestas referentes a: liderazgo y estrategia-personas y comunicación-responsabilidad y motivación- administración de riesgo e infraestructura.
	Integridad y valores éticos.	Existencia de código de ética y de procedimientos de comunicación de actos no éticos. Control del cumplimiento del código ética.
	Compromiso hacia la competencia.	Prácticas de educación formal (capacitación) y entrenamiento en la práctica.
	Estructura de la organización.	Asignación de autoridad, responsabilidad y delegación.
	Políticas y prácticas de RRHH.	Procesos de entrada y de salida del personal.
	Comités Directivos - Comité de Auditoría.	Comunicación y seguimiento de decisiones.

Establecimiento de Objetivos:	Objetivos estratégicos alineados a los Objetivos específicos de: operativos-financieros-cumplimiento.	Anualmente se realiza la planeación estratégica de la cual, las Gerencias Nacionales generan un documento en el que se detalla la misión-visión-principios morales-valores empresariales y en donde se determinan las metas de largo plazo y los objetivos del año.
Identificación de eventos:	Identificación de oportunidades y amenazas. Evaluando: factores internos: estructura-personal-procesos-tecnología; factores externos: económicos- políticos-sociales- tecnológicos- ambientales.	El anterior documento a su vez presenta un análisis FODA y el escenario: económico-político-regulatorio.
Evaluación del Riesgo:	Metodología para la evaluación del riesgo, evaluando probabilidad e impacto.	La organizaciones mantienen vigente la "Metodología para la elaboración de la Matriz de Riesgos de la Organización", en donde se define la medición del riesgo a través de un método de tratamiento de riesgo. En este se determinan escalas para valorar la probabilidad y el impacto, producto de lo cual se evalúa cada riesgo inherente en 5 categorías: Bajo-Moderado- Alto-Extremo- Extremo/Catastrófico y se determina la medida sugerida. Adicionalmente se determinan los controles que mitigan esos riesgos y se le da una valoración de eficacia a tales controles, para calcular el riesgo residual.
Respuesta al Riesgo:	Evitarlo- Reducirlo-Compartirlo-Aceptarlo Costo beneficio de la respuesta.	

Actividades de Control:	Políticas y procedimientos.	Se encuentran emitidas las principales políticas que norman los principales procesos de la organización y los flujos de procesos se encuentran diagramados.
	Controles sobre los sistemas: controles generales y de aplicación sobre actividades.	Los controles se detallan en los flujogramas de cada subproceso y en forma más detallada en la Matriz de Controles.
Comunicación:	Interna y externa: Características de la buena información: veraz -actualizada- oportuna-accesible.	
Monitoreo	Actividades permanentes.	Son las realizadas para realizar el monitoreo de la efectividad de los riesgos corporativos. Esto incluye la revisión de indicadores de gestión o indicadores de alerta.

	Evaluaciones independientes	Se mantienen las siguientes evaluaciones independientes realizadas por: -Auditoría interna de acuerdo al plan anual. -Auditoría externa que presenta anualmente: la opinión sobre los estados financieros- carta de control a la gerencia- informe de límites de crédito- informe sobre lavado de dinero- información financiera suplementaria- informe tributario. - Calificadoras de riesgos. - Auditoría de la SBS que presenta la evaluación sobre el alcance definido en su planificación. - Determinación tributarias realizadas por el SRI.

4.2. QUE ES LA METODOLOGÍA GREC, Y CUALES SON SUS FUNDAMENTOS CON RELACION AL RIESGO?

GREC es una metodología desarrollada por la Superintendencia de Bancos y Seguros del Ecuador (SBS) para efectuar una evaluación integral a las instituciones financieras del país, basado en un enfoque de riesgos, contempla un sistema de calificación denominado (GREC) por las áreas en las que se realiza la evaluación: gobierno corporativo, riesgos, evaluación financiera y cumplimiento.

Este modelo de supervisión bancaria enfoca la supervisión en:

- Un esquema de regulación efectiva y prudente, incluyendo normas de acceso a la actividad financiera como normas de ejercicio.

- Un sistema de supervisión permanente de las instituciones, integrado por la recepción de información periódica, e inspecciones in situ.

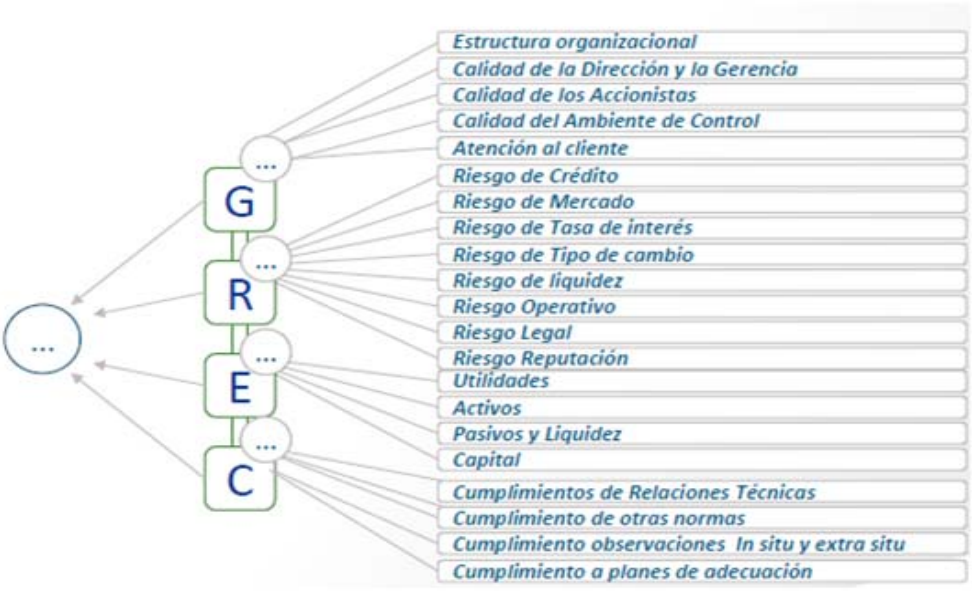
- Un conjunto de medidas de carácter corrector (formulación de requerimientos y recomendaciones)

Este método de evaluación está basado en riesgos dado que efectúa una supervisión según el perfil que tiene cada entidad, de manera continua y fundamentalmente es integrada ya que se coordina el

accionar de todas las áreas lo cual facilita y permite la detección oportuna de problemas.

Este proceso y enfoque estandarizado que integra a todas las áreas de la organización asegura estándares mínimos, así como modelos de reporte que define de manera clara y concreta las funciones y productos a entregar por las áreas de apoyo lo cual mejora la coordinación de las áreas y las formaliza. El elemento más importante que esta metodología aporta a este estudio sin lugar a dudas es el pasar del fuerte énfasis en "compliance" y del "check list" a la evaluación de los procesos así como a la identificación de potenciales deficiencias en los controles implementados con regulación efectiva y prudente.

Gráfico No. 1[5].



[5] Gráfico tomado del documento de fortalecimiento del proceso de supervisión de instituciones financieras de la Superintendencia de Bancos y Seguros del Ecuador.

4.3. PROCESO DE ADMINISTRACION DEL RIESGO USANDO UNA ADAPTACION METODOLÓGICA.

El proceso de adaptación plantea utilizar una metodología de trabajo guía basada en COSO – COBIT – GREC, con la finalidad de realizar evaluaciones de auditoría basadas en riesgos aplicando un enfoque sistemático y disciplinado para la evaluación de los procesos existentes en la organización priorizando la identificación de riesgos en general e identificando los requerimientos normativos locales e internacionales en torno a ellos y procurando un proceso de retroalimentación continuo que debe incluir:

Gráfico No. 2.

Fuente: PRICEWATERHOUSECOOPERS (2005) “Administración de Riesgos Corporativos – Marco Integrado”
Elaborado por: Andrés Aguayo Yépez.

- Evitar la ejecución de procesos que le convierten a la unidad de auditoría en juez y parte.

- Implementación de un marco metodológico generalmente aceptado como guía de trabajo considerando la matriz de riesgos institucional.

- Ajustar la planificación de auditoría considerando revisiones integrales con enfoque a riesgos.

- Mejorar la comunicación interna de resultados de auditoría

- Elaborar indicadores de gestión que permitan medir el desempeño de la unidad de auditoría.

El trabajo fundamental en este proceso de adaptación metodológica es definir la estrategia que se va a utilizar por el departamento de auditoría para la realización del trabajo, para ello es necesario partir de los objetivos y alcance previstos por el área considerando toda la información obtenida y conocimientos adquiridos sobre la entidad auditable, y para lograr aquello es necesario recabar la siguiente información:

Recolección de información de la organización:

- Planeación estratégica del año: que incluye un análisis FODAC, un análisis de la economía local y el impacto de la economía internacional, objetivos institucionales y los principales proyectos a desarrollarse.

- Planes de negocio de las principales líneas del negocio particular.
- Información financiera.
- Presupuestos.
- Actas de junta general de accionistas, actas de directorio, y actas de los diferentes comités: riesgos, crédito, cumplimiento, etc.
- El conocimiento acumulado del auditor sobre el funcionamiento del negocio, de acuerdo a la metodología creada para el efecto.

Evaluación de los factores de cambio en la organización:

- Regulaciones /economía.
- Personal nuevo y cambio de directivos principales.
- Sistemas de información nuevos o rediseñados.
- Crecimiento rápido.
- Tecnología nueva para producción.
- Nuevas líneas, productos o actividades.
- Reestructuraciones organizacionales.
- Operaciones en el exterior.
- Incorporación de la variable riesgo en todas las decisiones de negocio.
- Fusiones y/o adquisiciones.

Identificación de la Matriz de Riesgos Institucional emitida por el área de riesgos:

- Analizar la matriz de riesgo general y detallado por procesos.

- Establecer los procesos en donde existen riegos con valoración mayor a "Moderada[6]" determinados por el área de riesgos.

- Evaluar la aplicabilidad y funcionalidad de la matriz y sugerir cambios y modificaciones a la misma.

Utilización de factores de riesgo:

Los "Factores de Riesgo" son aquellas condiciones o particularidades con un alto grado de importancia para la organización y que son utilizados por Auditoría Interna para identificar la probabilidad de que ocurran eventos que puedan afectarlos adversamente, ya que constituyen una probabilidad medible, tienen valor predictivo y pueden usarse como variables de calificación para definir el nivel de riesgo de los entes auditables.

Con base en la literatura previa existente, en entrevistas preliminares y en estudios de pruebas efectuadas, se han compilado un total de 19 potenciales factores de riesgo de auditoría, esta lista de factores abajo detallados está relacionado con el riesgo o con la asignación de los recursos que posee la auditoría interna cuando el objetivo es minimizar las perdidas a su organización. Los resultados están detallados en orden de importancia en concordancia con el resultado de los estudios realizados[7]:

[6] Riesgo moderado considerado como pérdidas de reputación e imagen medias, pérdidas económicas medias.
[7] The Institute of Internal Auditors, Inc. "A framework for Evaluating Internal Audit Risk" Table 5- Free Translation.

Cuadro No. 4.

RISK FACTOR RANKED BY OVERALL MEDIAN RATING		
FACTOR RANKING	**FACTOR**	**MEDIAN RANK**
1	Calidad del sistema de control interno.	1.40
2	Competencia de la administración.	2.34
3	Integridad de la administración.	2.38
4	Unidad de medida (ingresos, activos)	2.65
5	Cambios recientes en los sistemas contables.	2.67
6	Complejidad de las operaciones.	2.79
7	Cambio reciente en personal clave.	2.83
8	Liquidez de activos.	2.84
9	Deterioro de las condiciones económicas departamentales.	2.90
10	Rápido crecimiento.	2.91
11	Extensión del procesamiento electrónico de datos.	3.00
12	Tiempo no auditado.	3.02
13	Nivel de presión de la administración para el logro de objeti	3.05
14	Extensión de las regulaciones gubernamentales.	3.26
15	Nivel de moral de empleados.	3.27
16	Planes de auditoría de auditores independientes.	3.35
17	Exposición política / Publicidad adversa.	3.67
18	Necesidad de mantener la apariencia de una auditoría interna independiente.	3.88
19	Grado de distancia de la administración.	4.63

Fuente: THE INSTITUTE OF INTERNAL AUDITORS (IAI)
Elaborado por: Andrés Aguayo Yépez.

4.4. TRATAMIENTO DEL RIESGO INHERENTE Y EL RIESGO RESIDUAL.

La administración del riesgo hace parte integral de los procesos gerenciales, ya que es un proceso multifacético, sus aspectos para ser bien entendidos requieren la conformación de un equipo multidisciplinario, es un proceso interactivo en continuo desarrollo[8].

[8] Estándar Australiano – Neozelandés AS/NZ 1360, administración del riesgo.

Los objetivos de tal administración del riesgo[9] a ser alcanzados unos de forma inmediata y otros a mediano y largo plazo son:

- Minimizar los efectos adversos de los riesgos buscando su costo mínimo mediante su identificación, medición y control.
- Supervivencia.
- Continuidad de las operaciones.
- Estabilidad de las ganancias.
- Crecimiento continuo.
- Responsabilidad social.
- Garantizar lo adecuado de los recursos posteriores a las pérdidas.
- Minimizar los costos de la materialización de los riesgos.
- Proteger a los empleados de lesiones y accidentes.
- Cumplir las obligaciones legales y contractuales.
- Eliminar las preocupaciones.
- Empoderamiento del recurso humano.

Por tanto, el análisis del riesgo consiste en escoger cual será la valoración de los riesgos como tal, ya sea en términos cualitativos, semi-cuantitativos o cuantitativos, dependiendo de la importancia o disponibilidad de la información. La selección de la opción de tratamiento más apropiada involucra balancear el costo de implementar cada control contra los beneficios que se derivan de ellos. En la mayoría de los casos, no existe una solución completa como solución de tratamiento de riesgos, se puede buscar una combinación de

[9] Revista internacional LEGIS de Contabilidad & Auditoria, de los riesgos de auditoría a los riesgos del negocio. El cambio del modelo, pág. 28-29 Samuel Alberto Mantilla.

opciones y una de ellas es buscar reducir la probabilidad de ocurrencia de un riesgo y con ello sus consecuencias, o transferir simplemente el riesgo, de aquí la necesidad de introducir los siguientes conceptos:

- El riesgo inherente, significa evaluar la consecuencia y probabilidad del riesgo que ignora los controles que están vigentes en una organización.

- El riesgo residual, es el margen o residuo del riesgo que puede darse a pesar de las medidas de tratamiento para la administración del mismo.

Es necesario tener claro que en términos de costo y complejidad, las evaluaciones cualitativas y semi-cuantitativas son las más prácticas y ejecutables para la determinación de la pérdida monetaria por riesgo. El análisis cualitativo en la generalidad de casos se utiliza cuando los datos numéricos son inadecuados para llevar a cabo un análisis cuantitativo, como es el caso puntual de este trabajo de investigación.

CAPITULO V

EL RIESGO OPERATIVO Y LOS PUNTOS VULNERABLES EN LAS TECNOLOGIAS DE INFORMACION.

La introducción de requerimientos específicos de capital por riesgo operacional es una de las mayores novedades aportadas por la normativa de mejores prácticas recomendadas por Basilea II.

Por supuesto no solo a nivel internacional sino a nivel nacional es considerado uno de los temas que mayor debate y controversias ha generado en el sector financiero sobre todo, que aunque conocedor de la importancia de efectuar una gestión por la existencia de este riesgo, avalada por el hecho de que las principales quiebras de entidades en los últimos años han sido producidas temas de riesgo operacional, se mostró escéptico a su imputación en capital, fundamentándose en la inexistencia de un mecanismo estandarizado para la medición del riesgo.

Basilea II ha dado un paso importante con la definición o conceptualización de riesgo operativo, definiéndolo como el riesgo de

pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal y los sistemas internos o bien de acontecimientos externos.

La ausencia de estándares en el sector, ha propiciado el desarrollo de tres métodos para el cálculo del mismo, recomendando a las entidades que vayan progresando hacia el más avanzado a medida que se desarrollen sistemas y prácticas de medición del riesgo operacional más sofisticados y más sensibles a su situación particular de riesgo.[10]

Para llegar a estas definiciones se ha tomado como base la documentación puesta a disposición por parte del Comité de Basilea a través de sus documentos, volantes y comunicaciones permanentes:

- Método Básico: se calcula el capital como el 15% del margen ordinario y se recomienda la aplicación de los "sound practices" (conjunto de principios para la correcta gestión del riesgo operacional definidos por Basilea).

- Método Estándar: se calcula el capital como un porcentaje establecido a aplicarse sobre el margen ordinario de las unidades de negocio. La aplicación de este método exige a las entidades la segregación de su margen ordinario en las ocho líneas de negocio definidas por Basilea (por ejemplo, Banca comercial).

[10] Por este motivo, aquellas entidades que decidan aplicar un método más sofisticado no podrán posteriormente acogerse a un modelo más sencillo. Asimismo y dentro de los supuestos establecidos por la norma, las entidades podrán optar por aplicar a determinadas líneas (o entidades jurídicas, zonas geográficas u otros criterios internos) el enfoque Avanzado y para otras los enfoques menos sofisticados (Básico o Estándar).

- Método Avanzado: por contraposición a los métodos anteriores en que se asume que el capital es un porcentaje determinado del margen ordinario aspecto este criticado por su excesiva simplicidad al asumir una relación directa entre ganancias y riesgo, el requerimiento de capital en este método será igual a la medida de riesgo generada por el sistema interno de medición del riesgo operacional de la entidad, mediante la utilización de una serie de modelos cuantitativos y cualitativos. La utilización de este método está en cualquier caso se sujeta a la aprobación del supervisor.

5.1. RIESGO OPERATIVO EN TI: BASE LEGAL ECUATORIANA Y SUS MEJORES PRÁCTICAS SEGÚN BASILEA.

A pesar de que las organizaciones generalmente reconocen que factores como fraudes, cambios inesperados en las regulaciones, desastres naturales o errores en los sistemas de información representan fuentes de incertidumbre relevantes, no existía una concepción de que éstos como un conjunto de factores puedan ser agrupados bajo una misma categoría denominada “Riesgo Operativo”.

El Comité de Basilea ha definido el riego operativo como “el riesgo de pérdida causada por falla o insuficiencia de procesos, personas y sistemas internos o por eventos externos” [11]

[11] Basel Committee on Banking Supervision, 2003.

La norma ecuatoriana prevé lo establecido en el Capítulo V "De la gestión del riesgo operativo", del Título X "De la gestión y administración de riesgos" del Libro I "Normas generales para la aplicación de la ley general de instituciones del sistema financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros, y en lo referente a riesgo operativo en las tecnologías de información establece: "Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones" [12]

A medida que las organizaciones aumentan su dependencia en las tecnologías de la información, nacen asuntos de importancia y uno de ellos es que probablemente un alto porcentaje de los controles internos claves para la organización son promovidos por la tecnología de información. Por ejemplo: la política de cualquier empresa bien organizada establece que antes de realizar cualquier pago a un proveedor se debe realizar una triple comprobación: la verificación de la documentación sustento de la transacción, misma que era posteriormente grabada y archivada.

[12] Conforme a lo establecido en el Capítulo V "De la gestión del riesgo operativo", del Título X "De la gestión y administración de riesgos" del Libro I "Normas generales para la aplicación de la ley general de instituciones del sistema financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros.

En la actualidad, esas comprobaciones son realizadas por el sistema (software) de planificación de recursos empresariales (ERP, en inglés) de la empresa. Para auditar este control de forma efectiva, un auditor debe ingresar a conocer los parámetros del sistema ERP para evaluar las reglas y tal configuración si quiere tener evaluar de manera objetiva el control. Esto requiere de desarrollar habilidades y procedimientos de auditoría totalmente distintos a los que se aplicaban en el proceso histórico que se basaba en la verificación de la documentación física.

Un tema adicional que aparece con frecuencia, cuando se planifica el universo de auditoría de tecnología de información, se refiere a la comprensión de la forma en que los controles tecnológicos se relacionan con la información financiera y contable, los fraudes y otros asuntos clave. Esto se puede percibir fácilmente cuando se evalúan los controles dentro de un sistema de aplicación (por ejemplo: los parámetros de la triple comprobación anteriormente referidos). Sin embargo, es mucho más difícil cuando se evalúan las tecnologías que dan soporte por nombrar un ejemplo. Si se supone que una empresa mantiene una conexión a internet, pero carece de filtros de seguridad para proteger la red interna, ¿la información financiera es incorrecta? ¿las operaciones se han visto afectadas? Son temas que sin lugar a dudas llaman nuestra atención y deben ser valorados con toda seriedad.

Se hace cada vez más difícil realizar una correlación a medida que existe mayor distancia entre la tecnología y las operaciones normales del giro del negocio.

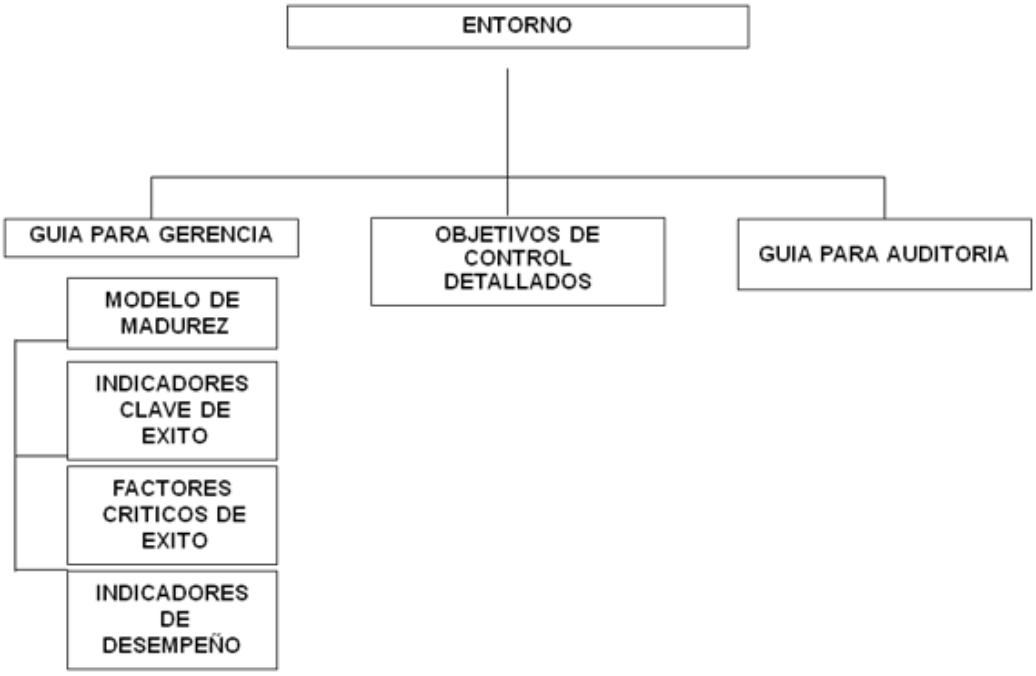
5.2. METODO DE TRABAJO COBIT, SUS DOMINIOS Y ÁREAS DE ENFOQUE.

Los controles de tecnología de la información soportan la gestión y el gobierno del negocio, y proporcionan controles generales y técnicos sobre las infraestructuras de tecnología de la información tales como: aplicaciones, información, infraestructura y personas, es por ello que el marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades[13].

Hay un método para realizar una gestión controlada y está explicado en el ENTORNO, hay un mínimo de controles que se deben implantar, y son los SUBOBJETIVOS DE CONTROL, hay una manera efectiva de auditar los controles, y está en la GUIA DE AUDITORIA y finalmente hay una manera de controlar la GESTION informática, y está en la GUIA PARA LA GERENCIA.

[13] IT Governance Institute, Cobit 4.1 - 2007

Gráfico No. 3.



Control Objetives for Information and Related Technology (COBIT, por su sigla en inglés), lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología de la información, vinculando tecnología informática y prácticas de control. COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para:

- La alta gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo - beneficio del control.

- Los usuarios finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

- Los auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar control mínimo requerido.

- Los responsables de TI: para identificar los controles que requieren en sus áreas.

- También puede ser usado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

En cada auditoria de sistemas de información, el auditor deberá diferenciar entre aquellos controles generales que afectan a todos los sistemas de información y aquellos que operan en un nivel más específico, con el fin de centrar los esfuerzos de la auditoria en las aéreas de riesgo relevantes para el objetivo de auditoría, entre las características más sobresalientes están:

- Orientado al negocio.
- Alineado con estándares y regulaciones “de facto”

- Basado en una revisión crítica y analítica de las tareas y actividades en TI.
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

La estructura de COBIT se define a partir de una premisa simple y pragmática: “Los recursos de las tecnologías de la información se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos”

COBIT se divide en tres niveles: dominios, procesos y actividades.

Dominios: agrupación natural de procesos normalmente corresponden a un dominio o a una responsabilidad organizacional.

Procesos: conjuntos o series de actividades unidas con delimitación o cortes de control.

Actividades: acciones requeridas para lograr un resultado medible.

COBIT define 34 objetivos de control generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro grandes dominios o clasificaciones de alto nivel que se detallan a

continuación junto con una descripción general de las actividades de cada uno[14]:

1. "Planear y organizar (PO): este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

2. Adquirir e implementar (AI): para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

3. Entregar y dar soporte (ER): este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.

[14] IT Governance Institute, Cobit 4.1 – 2007.

4. Supervisión (S): todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno".

5.3. COMO IDENTIFICAR PUNTOS VULNERABLES EN LA GESTION TECNOLÒGICA.

Una gestión de puntos vulnerables consiste en identificar los procesos y las tecnologías que una organización emplea para evaluar y solucionar las vulnerabilidades (entendidas como deficiencias en los sistemas de información) de TI (debilidades o exposiciones en los activos o procesos de TI que pueden generar un riesgo[15] de negocio o un riesgo de seguridad[16]).

Las nuevas tecnologías de la información (TI) están modificando indudablemente la naturaleza de la función de la auditoría interna, ya que a medida que surgen nuevos riesgos, se requieren nuevos procedimientos para identificarlos y gestionarlos adecuadamente. Para lograr entender que significa efectuar una gestión de puntos vulnerables, es necesario primero conocer que necesitan los miembros de los órganos de gobierno, los ejecutivos, los profesionales de TI y los auditores internos para tratar los temas de control de la tecnología y su impacto en el negocio y sobre todo en el bancario.

[15] Como por ejemplo, no poder mantener la integridad de los informes financieros o pérdida de ganancias o productividad.
[16] Como por ejemplo, violaciones a la confidencialidad, integridad o disponibilidad de datos.

Existen seis indicadores para la identificación de procesos deficientes de gestión de puntos vulnerables[17]:

- "Cantidad de incidentes de seguridad más alta que lo aceptable[18] durante un período dado.

- Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.

- Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.

- Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.

- Falta de un sistema de gestión de activos.

- Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades".

[17] THE INSTITUTE OF INTERNAL AUDITORS. (2006) "Guía de Auditoria de Tecnología Global (GTAG 6)" United States: 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201.

[18] La cantidad "aceptable" de incidentes se puede determinar comparando la tolerancia a la pérdida de uno, con la pérdida proveniente de incidentes de experiencias anteriores. De esta manera, uno puede ajustar los esfuerzos de gestión de puntos vulnerables balanceando los costos de implementar controles y enmendar vulnerabilidades con los beneficios de estas actividades, posiblemente como una función de pérdida que se evitó.

Una vez adquiridos los datos de las vulnerabilidades encontradas en los procesos internos, la organización debe poder determinar el riesgo real que estos representan, para ello es importante pasar a un segundo paso que es el de construir una matriz de riesgos.

El proceso de la gestión de puntos vulnerables propuesto implica[19]:

- "Identificación y validación a través de un inventario de activos que incluye: a) asegurarse de que se lleve y se mantenga un inventario de todos los sistemas de TI, b) asegurarse de que los sistemas de TI identificados estén agrupados y que se establezcan prioridades según sus riesgos de negocio correspondientes, y; c) asegurarse de que haya dependencias de proceso entre la gestión de configuración y la gestión del cambio.

- Evaluación de riesgos y establecimiento de prioridades, que requiere identificar los criterios utilizados para asignar los riesgos a medida que se detectan las vulnerabilidades, así como asegurarse de que los criterios se utilizan en forma coherente en toda la organización.

- Esquemas de supervisión que sirven para identificar los procesos automatizados y manuales para la detección de vulnerabilidades, y desarrollar planes de contingencia para el caso en que una vulnerabilidad identificada no reciba el control adecuado a tiempo.

[19] THE INSTITUTE OF INTERNAL AUDITORS. (2006) "Guía de Auditoria de Tecnología Global (GTAG 6)" United States: 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201.

- Mantenimiento y mejoras al asegurarse de que los activos de TI sean mantenidos en un formato estandarizado para ayudar a rastrear los elementos físicos y lógicos del activo de TI, como por ejemplo, modelos, aplicaciones instaladas y seguridades.

- Detección de vulnerabilidades al identificar herramientas automatizadas utilizadas para supervisar la red y asegurarse de que los activos de TI se revisen periódicamente. Identificar las fuentes utilizadas para la información de vulnerabilidades oportuna (por ejemplo, terceros, proveedores de software, etc).

- Establecer prioridades entre vulnerabilidades analizando de qué manera se cuantifica la importancia en función del impacto y criticidad del sistema. Asegurarse de que el impacto de negocio se incluya como un identificador de prioridad medible.

- Gestión de incidentes, los procedimientos de control deben ser coherentes en toda la organización. El impacto y la urgencia asignados a los denominados incidentes deben estar en línea con el riesgo de negocio del activo.

- Acuerdos de nivel de operaciones buscando que haya acuerdos de nivel de operaciones implementados para asegurarse que el ritmo de la gestión de puntos vulnerables y las entregas de procesos se midan y tengan una persona a cargo responsable.

- Validación de los hallazgos asegurándose de que hay un proceso implementado para identificar falsos positivos y negativos durante la detección. Asegurarse de que se analicen las vulnerabilidades según corresponda al entorno establecido.

- Gestión del cambio al analizar si los cambios son reactivos ante las vulnerabilidades identificadas. Los controles se deben planificar y probar antes de su implementación. Los cambios que se producen como resultado de vulnerabilidades deben ocasionar el mínimo grado de interrupciones en el negocio.

- Políticas y requerimientos de que los roles y las responsabilidades estén definidos para las funciones de identificación, comunicación y control. Identificar las políticas y los procedimientos para asegurarse de que se hayan definido las estrategias y las decisiones apropiadas".

5.4. MECANISMOS DE MEDICION DEL ROP Y PLANES DE TRATAMIENTO.

Las fuentes de información disponibles son importantes a la hora de determinar el tipo de metodología a utilizar para la medición del riesgo operativo, sin embargo el Comité de Basilea reconoce dos importantes categorías: los enfoques descendentes y los enfoques ascendentes.

Hoy en día, la mayoría de instituciones financieras importantes están empezando a utilizar metodologías ascendentes para la identificación y cuantificación del riesgo operativo. Este tipo de metodologías ese basan en modelos cuantitativos de dos tipos: modelos estadísticos y modelos causales, en donde los primeros se basan en información histórica sobre la frecuencia y el monto de los eventos de pérdida, mientras que los modelos causales, adicionalmente a la información histórica tienen en cuenta el juicio de expertos.

La escasez de información histórica sobre los eventos de pérdida debidas al riesgo operativo, ha generado el desarrollo de una metodología que tiene en cuenta la información cualitativa de una manera estructurada pero al mismo tiempo incorpora los eventos de pérdida a razón de riesgo operativo, en la medida que se vayan presentando. Esta metodología consta de nueve pasos y se describen de la siguiente manera[20]:

PASO 1: Seleccionar líneas de negocio; en este paso se seleccionan las líneas de negocio de la entidad que se van a tener en cuenta en la identificación y cuantificación de la exposición al riesgo operativo, es necesario además establecer un horizonte de tiempo dentro del cual se va a medir el nivel de exposición.

PASO 2: Categorizar los posibles eventos de pérdida; los eventos que generan posibles eventos de perdida definidos por el comité de Basilea

[20] UNIVERSIDAD DE LOS ANDES, A. Mendoza & M. Castillo. "Diseño de una metodología para la identificación del riego operativo en instituciones financieras" Bogotá-Colombia.

son: fraude interno; fraude externo; prácticas laborales y seguridad del ambiente de trabajo; prácticas relacionadas con los clientes, los productos y el negocio; daños a los activos físicos; interrupción del negocio por fallas en la tecnología de información; y deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

PASO 3: Definir niveles de severidad para los eventos de pérdida; se definen diferentes niveles de severidad para posibles eventos de pérdida de acuerdo con el monto de los mismos, se define tanto el número de niveles como el rango de valores asociados a cada nivel.

PASO 4: Identificar niveles de riesgo; los indicadores son variables que pueden alertar sobre la ocurrencia de eventos de pérdida.

PASO 5: Establecer la relación entre los eventos de pérdida y los indicadores de riesgo; se debe establecer un orden de importancia entre los indicadores de riesgo identificados para cada una de las categorías de eventos de pérdida, y de la misma manera se debe establecer la relación entre los eventos de pérdida y los indicadores de riesgo.

PASO 6: Construir un modelo de redes bayesianas; la construcción de este modelo se debe realizar en dos etapas: definición de variables y estimación de las probabilidades subjetivas.

PASO 7: Revisar las probabilidades subjetivas en la red bayesiana; este paso sirve para revisar las probabilidades condicionales que deben generarse en el paso anterior, tomando en cuenta la información histórica existente sobre los eventos de pérdida internos y externos.

PASO 8: Obtener la distribución de pérdida; para cada una de las categorías se debe establecer el número de operaciones o transacciones en los que podrían ocurrir eventos de pérdida durante el horizonte de tiempo establecido en el primer paso.

PASO 9: Calcular la provisión total; en este paso se suman las provisiones calculadas para cada una de las líneas de negocio, obteniendo la provisión total que debe hacer la entidad para cubrir posibles eventos de pérdida.

El riesgo es un concepto utilizado para expresar inquietudes acerca de los probables efectos de un entorno incierto, como el futuro es desconocido, cualquier rango de acontecimientos podría tener un impacto significativo en las metas y los objetivos de una organización, es por ello que la gestión de riesgos cierra el círculo tomando decisiones sobre la manera de abordar (tratamiento) los riesgos evaluados, y son:

- Evitar el riesgo: diseñando el proceso para eliminar riesgos en particular, minimizar los riesgos o cambiar la naturaleza de los riesgos que deban enfrentarse.

- Controlar el riesgo: instituir procedimientos para controlar el proceso que minimice las consecuencias y la severidad de los riesgos que se provoquen, lo cual incluye aceptar algo de riesgo.

- Compartir el riesgo: mediante convenios contractuales con proveedores, clientes, miembros constituyentes o terceros (tales como compañías aseguradoras), distribuyendo algo de riesgo o de las actividades de riesgo entre los demás y aceptando el restante.

Siempre existe una cantidad de riesgo residual que queda después de todos los esfuerzos realizados para evitar, controlar y compartir el riesgo. Si el riesgo residual es demasiado alto no debe realizarse la tarea, mientras que si el riesgo residual no es demasiado alto, la gerencia puede elegir aceptar esta cantidad de riesgo para alcanzar los objetivos. Además de los riesgos residuales que quedan después de los esfuerzos de gestión, existen riesgos inherentes en el proceso de administración conocidos como riesgo de control, o aquellos riesgos asociados con confiar en un procedimiento de control, etc, que no logra llevar a cabo su tarea.

Tanto el riesgo residual como el riesgo de control deben explícitamente abordar la administración del proyecto.

CAPITULO VI

CASO DE APLICACIÓN: MODELACIÓN DE LA ADAPTACION METODOLÓGICA.

6.1. MATRIZ DE RIESGO OPERATIVO EN LOS PROCESOS DE TI DE GESTION TECNOLÓGICA.

Para el desarrollo del caso práctico de aplicación es necesario comenzar manifestando que se efectuó un trabajo de recopilación de información con personal experto del área de tecnología, con el cual se pudo definir cuáles son los procesos relevantes dentro del universo de tecnología de información, para sobre tales procesos y subprocesos definir un mecanismo de medición de vulnerabilidad del proceso y posteriormente una medición cualitativa del riesgo inherente asociado a estos procesos.

Para ello es importante primero conocer que es una matriz de riegos y cuales son componentes de tal forma que una persona que no tenga el suficiente conocimiento en estos temas, logre comprender el estudio realizado, por tanto una matriz de riesgos se define como una herramienta de control y gestión utilizada para identificar los riesgos

inherentes relacionados con los subprocesos, procesos y macroprocesos. Evalúa la efectividad de una adecuada gestión y administración de riesgos que podrían impactar negativamente los objetivos de la institución por supuesto con la generación de pérdidas no solo económicas sino de reputación e inclusive afectando y poniendo en riesgo su continuidad como negocio en marcha.

La matriz de riesgos permite identificar la probabilidad de ocurrencia de un evento y el impacto en cada uno de los procesos de la organización.

La valorización de los riesgos se realiza en términos cualitativos, semi-cuantitativos o cuantitativos, teniendo en cuenta la calidad y la disponibilidad de información. Las evaluaciones cuantitativas y semi-cuantitativas son las más prácticas, sin embargo la información cualitativa se utiliza cuando los datos numéricos son incompletos para llevar a cabo un análisis cuantitativo como es el caso práctico desarrollado en este estudio.

A continuación se presenta un ejemplo de una matriz de riesgos para mejor comprensión:

Cuadro No. 5.

MATRIZ DE RIESGOS

		1	2	3	4	5
	Probab/Impacto	Insignificante	Menor	Moderado	Mayor	Catastrófico
5	Casi Certera	Alto	Alto	Extremo	Extremo	Extremo
4	Probable	Moderado	Alto	Alto	Extremo	Extremo
3	Posible	Bajo	Moderado	Alto	Extremo	Extremo
2	Improbable	Bajo	Bajo	Moderado	Alto	Extremo
1	Rara	Bajo	Bajo	Moderado	Alto	Alto

Elaborado por: Andrés Aguayo Yépez.

Es importante efectuar una diferenciación entre la probabilidad probable definida como la probabilidad de que no ocurra un evento en un mes pero si al menos una vez en tres meses. Y la probabilidad posible definida como la probabilidad casi cierta de que ocurra un evento al menos una vez al mes.

Estos conceptos y escalas de calificación son las que mejor se adaptan al estudio desarrollado y definen de mejor manera a la variable "frecuencia de ocurrencia de eventos" medidos en número de veces, estos conceptos han sido comprendidos de esta manera sobre la base de la Norma Australiana AS/AZS 4360:1999 sobre el manejo de riesgos.

Los beneficios de contar con una matriz de riesgo a nivel institucional permiten generar un instrumento de fácil manejo ya que presenta características de visualización que otras herramientas no poseen, permite ser utilizada por herramientas computacionales, que facilitan su uso en organizaciones con exposiciones a pérdidas múltiples y con alta variabilidad, además facilita la evaluación de los riesgos al identificar

aquellos que son prioritarios, con la finalidad de aplicar controles y preparar o diseñar planes de prevención.

El proceso de adaptación metodológica planteado en este estudio y el paso de construir la matriz de riesgo operativo en los procesos de tecnología de información planteado en esta investigación está basado en los siguientes estándares internacionales:

- Norma Australiana AS/AZS 4360:1999 sobre el manejo de riesgos.
- Metodología COSO, para la estructura conceptual de la gestión de riesgos.
- Acuerdo de Capitales “Basilea II”

Ahora bien, el estudio se ha enfocado en evaluar los procesos de tecnología, ya que son aquellos que no han sido considerados normalmente por las organizaciones y hasta podrían haber sido descuidados bajo el criterio de que estos son automatizados y no susceptibles de error humano en el procesamiento de la información como tal, para entender esto a continuación se aclara de mejor forma que controles tienen las herramientas tecnológicas.

Los controles de tecnología pueden ser clasificados como controles generales (aquellos controles de procesamiento organizacional) y controles de aplicación (aquellos controles de un sistema en particular dentro de la organización) esta diferenciación entre ellos es importante

ya que ayuda a enfocar el esfuerzo de auditoría en riesgos relevantes al objetivo de la auditoria como tal, para ello es necesario primero entender cómo se encuentra diseñado un esquema de tecnología en una organización.

El uso de computadoras en sistemas de información empresarial tienen efectos fundamentales sobre la naturaleza de las transacciones realizadas, los procedimientos seguidos, los riesgos que se corren y los métodos para aminorar tales riesgos, para ello a continuación se presenta una ilustración basada en las mejores prácticas de cómo debería ser una adecuada estructura tecnológica que parte de: la identificación de las áreas funcionales, el establecimiento de políticas y procedimientos, el reconocimiento de las necesidades de intercambio de información, los sistemas y los aplicativos necesarios para visualizar tal información de manera efectiva y eficiente, el almacenamiento y archivo de los datos asegurando y garantizando integridad en los mismos, y finalmente los sistemas operativos que se van a utilizar tomando en cuenta que deben ser concordantes con el espacio físico, la infraestructura y la capacidad económica de la organización.

Cuadro No. 6

Este esquema planteado de cómo debería estar conformado un departamento de tecnología basado en las mejores prácticas, posee funciones claves que incluyen: al administrador, al programador, al administrador de red y al operador de base de datos de análisis de sistemas, esta información es importante tenerla en cuenta ya que los procesos de gestión tecnológica definidos en el alcance del estudio a ser evaluados y desarrollados en la matriz de riesgos incluyen estas funciones en sus procesos y subprocesos, sobre esa base es necesario conceptualizar que es la gestión de tecnología.

LA GESTIÓN TECNOLÓGICA.

La gestión tecnológica abarca muchas áreas del mundo tecnológico sin embargo en este estudio nos enfocaremos en los sistemas de gestión de seguridad de los sistemas y la información.

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. La necesidad imperante del flujo de información y el traslado de recursos de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación y toda la información que contienen sus nodos[21]. Estos riesgos tecnológicos tienen impactos mayores a nivel de la organización ya que la pérdida de información relevante puede ocasionar impactos financieros sumamente importantes para el negocio y para su normal funcionamiento, tanto en el aspecto económico produciendo grandes pérdidas de dinero como en los efectos desencadenantes a nivel reputacional.

Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades.

[21] Un nodo es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar. Por ejemplo: en una red de ordenadores cada una de las máquinas es un nodo, y si la red es internet, cada servidor constituye también un nodo.

Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques cibernéticos externos a los que se expone defina una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización.

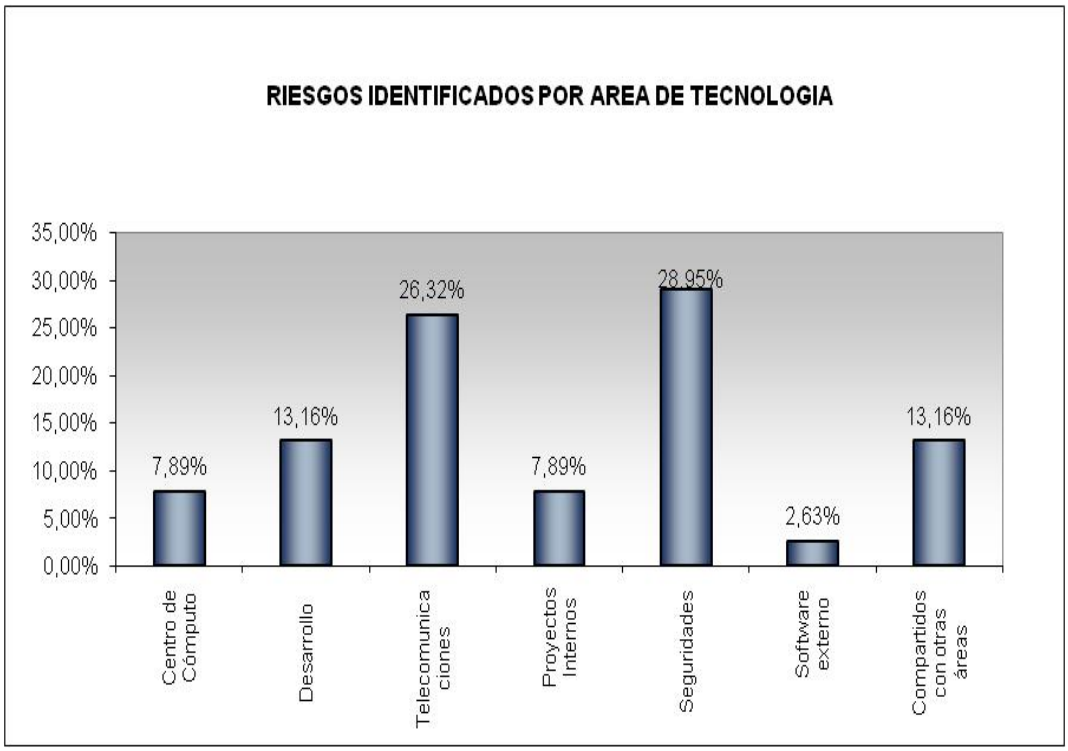
Al efectuarse una valoración cualitativa del nivel de riesgo que tienen los procesos de gestión tecnológica bajo el esquema planteado, se da un primer paso para en base a este análisis y la obtención de la data correspondiente lograr determinar en el futuro una valoración cuantitativa del riesgo.

Adicionalmente, el consejo para la práctica 2130.A1-2 del Marco Internacional para la práctica profesional de la auditoría interna, en cuanto al enfoque de privacidad de una organización señala: "*la actividad de auditoría debe evaluar la adecuación y eficacia de los controles en respuesta a los riesgos del gobierno, operaciones y sistemas de información de la organización, respecto de lo siguiente: fiabilidad e integridad de la información financiera y operativa, eficacia y eficiencia de las operaciones y programas, protección de activos, y cumplimiento de leyes, regulaciones, políticas, procedimientos y contratos."*

A continuación se presenta un detalle de algunos indicadores relevantes para un mejor entendimiento de la importancia del área de tecnológica

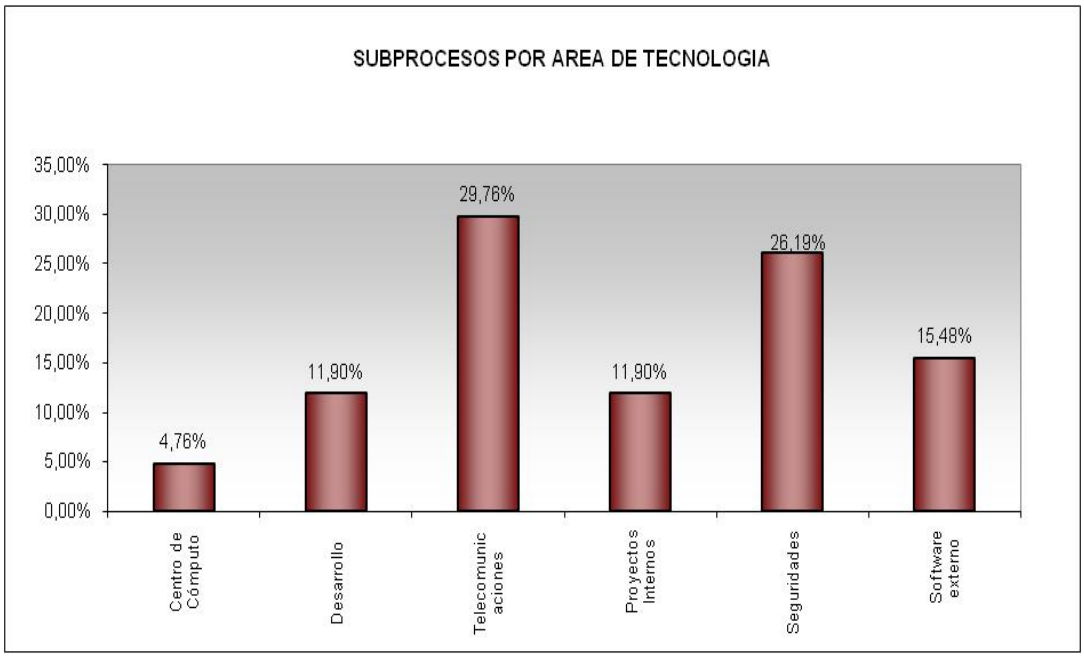
en una institución financiera, los datos han sido tomados de una institución financiera nacional, y constituyen un referente para poder identificar la importancia de hacer evaluación de riesgos a los procesos de tecnología.

Gráfico No. 4.



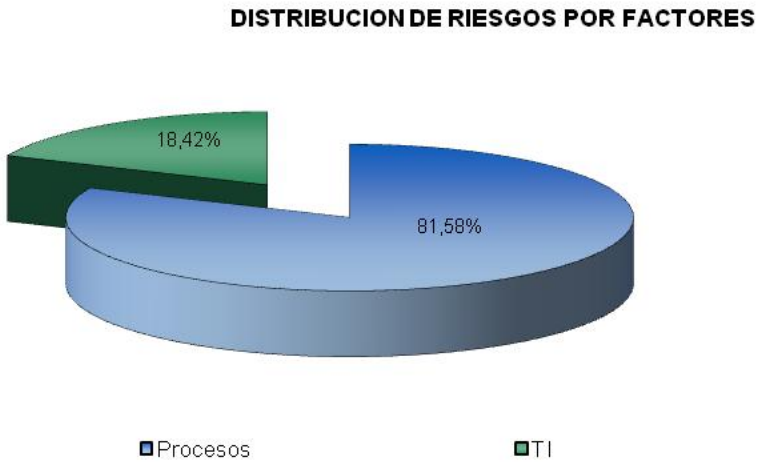
Fuente: INSTITUCIÓN FINANCIERA NACIONAL – INVESTIGACION 2011.
Elaborado por: Andrés Aguayo Yépez.

Gráfico No. 5.



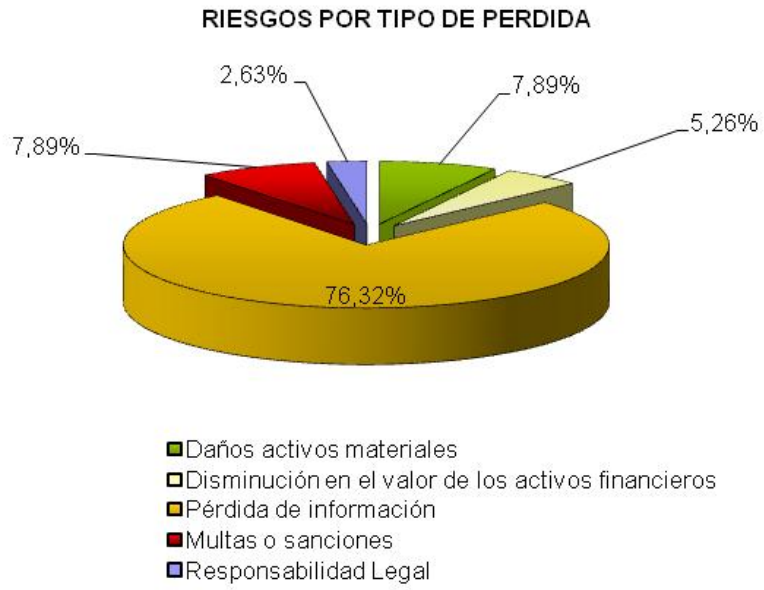
Fuente: INSTITUCIÓN FINANCIERA NACIONAL – INVESTIGACION 2011.
Elaborado por: Andrés Aguayo Yépez.

Gráfico No. 6.



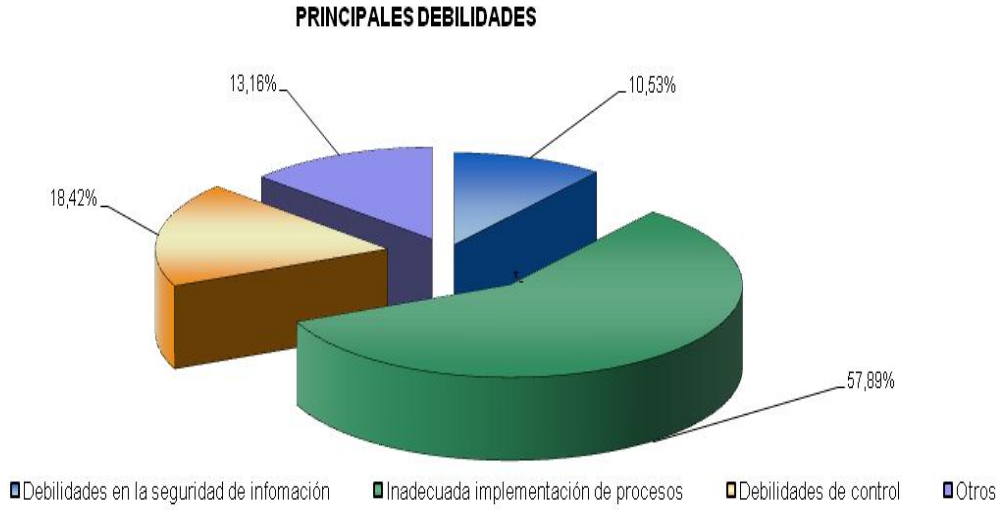
Fuente: INSTITUCIÓN FINANCIERA NACIONAL – INVESTIGACION 2011.
Elaborado por: Andrés Aguayo Yépez.

Gráfico No. 7.



Fuente: INSTITUCIÓN FINANCIERA NACIONAL – INVESTIGACION 2011.
Elaborado por: Andrés Aguayo Yépez.

Gráfico No. 8.



Fuente: INSTITUCIÓN FINANCIERA NACIONAL – INVESTIGACION 2011.
Elaborado por: Andrés Aguayo Yépez.

Dada la información anterior es indudable que la mayor cantidad de riesgos identificados en el área de tecnología de la información se encuentran en las telecomunicaciones, en las seguridades y en los trabajos de desarrollo, información que coincide con la cantidad de subprocesos que se manejan en dichos procesos, esto es importante conocer y evaluar para un departamento de auditoría con la finalidad de identificar puntos significativos de riesgo y es lo que lleva a este estudio a profundizar en esta área específica de la organización.

El análisis de distribución de riesgos (gráfico No.6) muestra que más del 80% del universo de riesgos se encuentran centralizados en los procesos, de ahí la importancia de establecer una matriz de riesgos a nivel de procesos y subprocesos con la finalidad de establecer un nivel real de riesgo como se lo ha realizado en este estudio (ver anexo No.2), se hace evidente también que la pérdida de información (gráfico No.7) es la causal más significativa de pérdidas para las organizaciones con un 76.32%. Finalmente se evidencia una relación muy directa entre el nivel de riesgo en los procesos y subprocesos con su inadecuada implementación (gráfico No.8) ya que este último se presenta como una de las principales debilidades en TI con un 57.89%.

Sobre la base de esta información preliminar, la interacción y participación del personal experto en el área de tecnología con quien se efectúo reuniones de trabajo a manera de entrevistas y asesoría, la documentación recopilada emanada de las mejores prácticas tanto de evaluación de riesgos como del tratamiento de las tecnologías de

información se determina que los procesos más importantes a ser evaluados en el presente estudio son los siguientes: a) administración de infraestructura, b) desarrollo mantenimiento e implementación de software, c) gestión de seguridad de información, d) gestión de soporte a usuarios, e) monitoreo de sistemas y aplicaciones, y f) procesamiento tecnológico; pero claro, previo a desarrollar el trabajo práctico es necesario una vez más conceptualizar estos procesos que van a ser evaluados para poder comprender que objetivo persigue cada uno y cuán importante es para la organización, la base de estos conceptos han sido tomados de la metodología COBIT que es el marco de referencia citado para evaluar los procesos de TI.

Administración de infraestructura:

Su objetivo es facilitar una disponibilidad mayor del sistema informático de la compañía, minimizar los problemas en producción y, en caso de darse éstos, poder resolverlos de forma más rápida.

Este proceso debe asegurar la integridad de las configuraciones de hardware y software de la compañía. Requiere como punto de partida tener y mantener un repositorio preciso y completo de todos los elementos de infraestructura. El proceso incluye el inventario de la configuración, establecer líneas base de la interrelación de los elementos y su operación conjunta, verificar y auditar la documentación y operación y mantener actualizada la información del repositorio.

Desarrollo mantenimiento e implementación de software:

Su objetivo es soportar de forma adecuada las operaciones del negocio mediante las aplicaciones automáticas correctas.

El proceso busca asegurar que las aplicaciones están a disposición del negocio, en línea con él. Cubre el diseño de las aplicaciones desde los requerimientos del negocio, la inclusión de controles y requisitos de seguridad en las mismas, y el desarrollo y configuración en línea con los estándares definidos, así como su implantación.

Gestión de seguridad de información:

Su objetivo es proteger todos los activos de información a fin de minimizar el impacto al negocio de las vulnerabilidades e incidentes de seguridad.

La necesidad de mantener la integridad de la información y proteger los activos requiere un proceso de administrar la seguridad.

El proceso incluye: establecer y mantener roles y responsabilidades por la seguridad de la tecnología, políticas, estándares y procedimientos. La administración de la seguridad incluye también realizar el monitoreo y pruebas periódicas, e implementar acciones correctivas para las vulnerabilidades detectadas y los incidentes ocurridos.

Gestión de soporte a usuarios:

Su objetivo es aumentar la productividad a través de la resolución rápida de cuestionamientos de usuarios, y esto de forma sostenible mediante los análisis de causa raíz y el estudio de las tendencias.

El proceso busca responder de forma oportuna y efectiva a las consultas y problemas de los usuarios. El punto base es un sistema o función que contemple el registro de la consulta o problema, el escalamiento de los problemas, un análisis de causa raíz y de tendencias de problemas y finalmente su resolución.

Monitoreo de sistemas y aplicaciones:

Su objetivo es asegurar que se están realizando las acciones tecnológicas correctas y en línea con las directivas del negocio.

El proceso incluye la definición de indicadores de desempeño, reportes sistemáticos y oportunos del desempeño, y acciones oportunas cuando hay desvíos.

Procesamiento tecnológico:

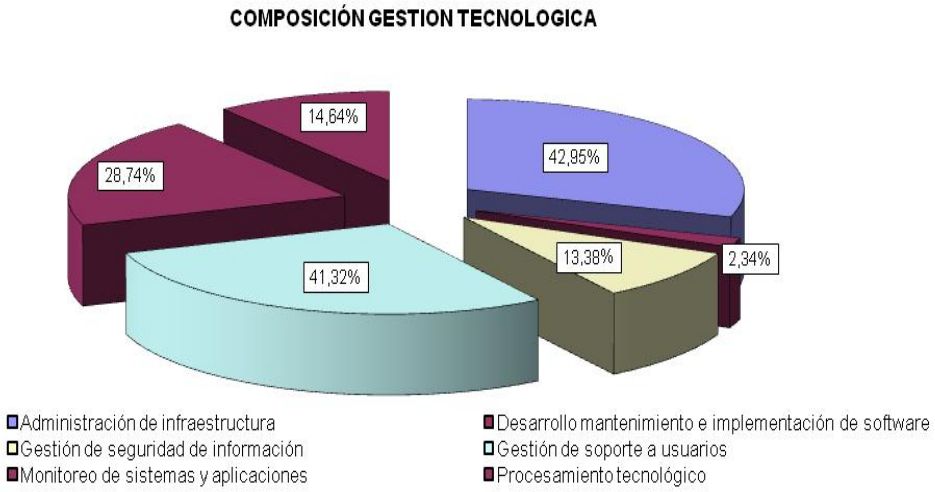
Su objetivo es ayudar a mantener la integridad de la data, que el negocio no sufra atrasos en sus actividades y reducir los costos operativos de tecnología.

El proceso busca un procesamiento completo y preciso de los datos, y un marco de mantenimiento diligente del hardware. Incluye definir políticas de procesamiento con procedimientos que administren un procesamiento ordenado, planificado, que proteja las salidas e interfases de información sensible, monitoree el desempeño de la infraestructura y asegure el mantenimiento preventivo del hardware.

CASO DE APLICACIÓN (1era parte - determinación del proceso vulnerable)

El siguiente cuadro elaborado sobre la base de la información obtenida en una institución financiera del país tomada como referencia para efectos de esta investigación, muestra la cantidad de transacciones ejecutadas en cada proceso de gestión tecnológica, que nos lleva a encaminar los esfuerzos de evaluación con mayor detenimiento a los procesos de: administración de infraestructura (42.95% del total de transacciones), gestión de soporte a usuarios (41.32% del total de transacciones) y procesamiento tecnológico (28,74% del total de transacciones), es decir estos procesos tienen mayor riesgo operativo.

Gráfico No. 9



INSTITUCIÓN FINANCIERA NACIONAL – INVESTIGACION 2011.
Elaborado por: Andrés Aguayo Yépez.

Los seis procesos descritos en el cuadro anterior (gráfico No.9) y bajo la metodología para identificación de vulnerabilidades propuesto en este trabajo son detallados a manera de matriz en el **anexo No.1** donde lo que se efectuado es identificar con el personal experto en TI los subprocesos relevantes de cada proceso para ser evaluados en función de los parámetros de detección de vulnerabilidades (5 parámetros recomendados por las mejores prácticas) en donde a nuestro criterio profesional determinamos que si algún subproceso no cumple con cualquiera de los parámetros antes mencionados, será valuado como proceso vulnerable, claro está que para llegar a esta categorización se obtuvo evidencia visual en el campo, así como se efectuó indagaciones con el personal que realiza estas actividades (entrevistas con personal clave), y por supuesto con la cantidad de requerimientos atendidos a las

actividades ejecutadas en estos subprocesos, todo esto complementó nuestro criterio profesional de valuación.

Resultado de la valoración del proceso de administración de infraestructura: Este proceso contiene subprocesos considerados vulnerables bajo el esquema planteado de valoración, por tanto tiene riesgo operativo y requiere que se determine un nivel de impacto y probabilidad mismo que es desarrollado en el anexo No.2.

A continuación se presenta un cuadro resumen de la valoración cualitativa, el detalle completo del trabajo desarrollado se presenta en el anexo No.1.

Cuadro No. 7.

Macroproceso	Proceso	Subprocesos	Subproceso es vulnerable?
Gestión de Tecnología	Administración de Infraestructura	Administración y monitoreo de accesos remotos	SI
Gestión de Tecnología	Administración de Infraestructura	Administración y monitoreo de equipos de la red WAN y equipos de comunicaciones	SI
Gestión de Tecnología	Administración de Infraestructura	Administración, monitoreo y diseño de funcionamiento de servidores para revisión de logs	SI
Gestión de Tecnología	Administración de Infraestructura	Compactación de bases correo electrónico	SI
Gestión de Tecnología	Administración de Infraestructura	Diseño de soluciones de comunicaciones	SI
Gestión de Tecnología	Administración de Infraestructura	Disponibilidad de memoria RAM	SI
Gestión de Tecnología	Administración de Infraestructura	Disponibilidad de procesador	SI
Gestión de Tecnología	Administración de Infraestructura	Monitoreo y administración de centrales telefónicas	SI
Gestión de Tecnología	Administración de Infraestructura	Revisión de espacio disponible y de uso de los discos duros	SI

(PO)	Planear y Organizar

Elaborado por: Andrés Aguayo Yépez.

Resultado de la valoración del proceso de desarrollo mantenimiento e implementación de software: Este proceso contiene subprocesos considerados vulnerables bajo el esquema planteado de valoración, por tanto tiene riesgo operativo y requiere que se determine un nivel de impacto y probabilidad mismo que es desarrollado en el anexo No.2.

A continuación se presenta un cuadro resumen de la valoración cualitativa, el detalle completo del trabajo desarrollado se presenta en el anexo No.1.

Cuadro No. 8.

Macroproceso	Proceso	Subprocesos	Subproceso es vulnerable?
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Atención de requerimientos de tecnología	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de facturación	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de ambientes	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Pruebas técnicas y de certificación	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a producción	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a pruebas	SI

(DS)	Entregar y Dar Soporte

Elaborado por: Andrés Aguayo Yépez.

Resultado de la valoración del proceso de gestión de seguridad de información: Este proceso contiene subprocesos considerados vulnerables bajo el esquema planteado de valoración, por tanto tiene riesgo operativo y requiere que se determine un nivel de impacto y probabilidad mismo que es desarrollado en el anexo No.2.

A continuación se presenta un cuadro resumen de la valoración cualitativa, el detalle completo del trabajo desarrollado se presenta en el anexo No.1.

Cuadro No. 9.

Macroproceso	Proceso	Subprocesos	Subproceso es vulnerable?
Gestión de Tecnología	Gestión de Seguridad de Información	Administración de usuarios	SI
Gestión de Tecnología	Gestión de Seguridad de Información	Administración y autenticación de backups internos y externos	SI
Gestión de Tecnología	Gestión de Seguridad de Información	Procedimiento de control de cambios	SI
Gestión de Tecnología	Gestión de Seguridad de Información	Procedimiento para reprocesos	SI

(ME)	Monitorear y Evaluar

Elaborado por: Andrés Aguayo Yépez.

Resultado de la valoración del proceso de gestión de soporte a usuarios:

Este proceso contiene subprocesos considerados vulnerables bajo el esquema planteado de valoración, por tanto tiene riesgo operativo y requiere que se determine un nivel de impacto y probabilidad mismo que es desarrollado en el anexo No.2.

A continuación se presenta un cuadro resumen de la valoración cualitativa, el detalle completo del trabajo desarrollado se presenta en el anexo No.1.

Cuadro No. 10.

Macroproceso	Proceso	Subprocesos	Subproceso es vulnerable?
Gestión de Tecnología	Gestión Soporte a Usuarios	Atención de requerimientos	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Atención helpdesk	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Atención requerimientos WEB	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Creación de usuarios de correo electrónico	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Eliminación de usuarios de correo electrónico	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Entrega de reportes por requerimiento de usuario	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Generación de informes	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Preparación de equipos	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Revisión de actualización del sistema operativo	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Revisión de definiciones antivirus	SI

(AI)	Adquirir e Implementar

Elaborado por: Andrés Aguayo Yépez.

Resultado de la valoración del proceso de monitoreo de sistemas y aplicaciones y procesamiento tecnológico:

Este proceso contiene subprocesos considerados vulnerables bajo el esquema planteado de valoración, por tanto tiene riesgo operativo y requiere que se determine un nivel de impacto y probabilidad mismo que es desarrollado en el anexo No.2.

A continuación se presenta un cuadro resumen de la valoración cualitativa, el detalle completo del trabajo desarrollado se presenta en el anexo No.1.

Cuadro No. 11.

Macroproceso	Proceso	Subprocesos	Subproceso es vulnerable?
Gestión de Tecnología	Monitoreo de Sistemas y Aplicaciones	Monitoreo de servicios, sistemas y aplicaciones	SI
Gestión de Tecnología	Procesamiento Tecnológico	Parametrizaciones	SI
Gestión de Tecnología	Procesamiento Tecnológico	Procesamiento de transacciones y disponibilidad de información	SI
Gestión de Tecnología	Procesamiento Tecnológico	Seguimiento y paso a producción	SI

(DS)	Entregar y Dar Soporte
(ME)	Monitorear y Evaluar

Elaborado por: Andrés Aguayo Yépez.

6.2. ASIGNACION DE NIVELES DE RIESGO A TRAVÉS DE LA DETERMINACIÓN DE FACTORES DE RIESGO.

CASO DE APLICACIÓN (2da parte – instructivo para la medición del riesgo operativo previo a la construcción de la matriz de riesgo)

La premisa principal para asignar "factores de riesgo[22]" para la determinación del nivel de riesgo real que poseen los procesos y subprocesos está basada en que la actividad de auditoría interna dentro de sus funciones está la de asistir a la organización mediante la identificación y evaluación de las exposiciones significativas a los riesgos y la contribución a la mejora de los sistemas de gestión de riesgos y control, de ahí la necesidad de construir una matriz de riesgos determinando factores sobre la base del criterio y juicio profesional del auditor.

Para ello es de vital importancia hacer referencia al marco internacional para la práctica profesional de la auditoría interna 2120-1 que establece: ***"La gestión de riesgos es una responsabilidad clave de la alta dirección y el consejo de administración. Para cumplir sus objetivos de negocio, la dirección asegura que existen y funcionan sólidos procesos de gestión de riesgos. Los consejos de administración cumplen una función de supervisión para determinar que existan apropiados procesos de gestión de riesgos y que estos procesos sean adecuados y eficaces. En este rol,***

[22] Constituyen una probabilidad medible, tienen valor predictivo y pueden usarse como variables de calificación para definir el nivel de riesgo de los entes auditables.

pueden dirigir a los auditores internos a que los ayuden mediante el examen, evaluación, informe y recomendación de mejoras sobre la adecuación y eficacia de los procesos de gestión de riesgos de la dirección"

INSTRUCTIVO BASADO EN EL MARCO METODOLOGICO COSO-ERM, COBIT Y GREC PARA MEDIR CUALITATIVAMENTE EL RIESGO OPERATIVO EN LOS PROCESOS DE GESTION TECNOLOGICA.

El proceso de evaluación de riesgos es muy complejo, sin embargo como parte de los planes para llevar a cabo las responsabilidades del departamento de auditoría, creemos es conveniente desarrollar un instructivo que genere pautas a ser tomadas en cuenta para una eficaz identificación y medición del riesgo, a continuación el desarrollo de la propuesta:

1) Identificación de las actividades auditables a través de la construcción de la matriz de riesgos.
2) Identificación y valoración de los factores de riesgo que son relevantes a las actividades auditables.
3) Ponderación de los factores de riesgo (impacto y probabilidad), y;
4) Determinación de niveles de criticidad de cada subproceso.

PASO 1: IDENTIFICACIÓN DE LAS ACTIVIDADES AUDITABLES

La primera fase del proceso de valoración de riesgos es la identificación de las actividades auditables y dichas actividades conciernen a aquellos sujetos, unidades o sistemas que son capaces de ser definidos y evaluados, para el caso de estudio estos entes auditables son los procesos de tecnología de la información valorados y considerados como vulnerables: administración de infraestructura, desarrollo mantenimiento e implementación de software, gestión de seguridad de información, gestión de soporte a usuarios, monitoreo de sistemas y aplicaciones, y procesamiento tecnológico, por supuesto estos subprocesos salieron de un “Inventario de procesos y subprocesos institucional”

Como auditores internos, contamos con la ventaja de contar con el conocimiento, tanto de los objetivos de la entidad a la cual pertenecemos, como de las actividades que ésta realiza para lograrlos; asimismo, tenemos a nuestro alcance los medios, información, documentación, experiencia de revisiones anteriores, que constituyen los elementos necesarios que nos ayudan como departamento para adoptar dos importantes decisiones:

- Establecer el área y los subprocesos a los cuales estarán dirigidos los esfuerzos y recursos de auditoría como en este caso son los subprocesos de tecnología de la información, y;

- Determinar qué aspectos claves serán evaluados dentro de cada auditoría que se plantea efectuar.

PASO 2: IDENTIFICACIÒN Y VALORACIÓN DE LOS FACTORES DE RIESGO QUE SON RELEVANTES PARA LAS ACTIVIDADES AUDITABLES:

Los factores de riesgo son el criterio usado para identificar el significado relativo de, y probabilidad que, condiciones y/o eventos puedan ocurrir que puedan afectar adversamente a la organización. Para esto se ha definido en este estudio considerar los siguientes factores de riesgo:

- Calidad del sistema de control interno a través de la matriz de riesgos institucionales.
- Complejidad de las operaciones e impacto en los procesos críticos de la organización.
- Nivel de presión de la administración para el logro de objetivos estratégicos.
- Resultado de auditorías independientes anteriores.
- Impacto en lavado de activos, exposición política y publicidad adversa.
- Tiempo no auditado.

a) Calidad del sistema de control interno a través de la matriz de riesgos institucionales, de tal manera que se pueda verificar que la Administración ha identificado y conoce los riesgos a los que está expuesta su organización en sus diferentes procesos y subprocesos y los controles que ha implementado para el efecto.

Cuadro No. 12.

Factores de Riesgo	Nivel de Impacto	Valoración	Descripción del Nivel de Impacto
Calidad del sistema de control interno a través de la matriz de riesgos institucionales	Bajo	1	Menores efectos que pueden ser fácilmente remediados. Si el riesgo es bajo se administra con procedimientos rutinarios, si es insignificante no requiere ninguna acción.
	Moderado	2	Riesgo moderado y aceptable debe ser administrado con procedimientos normales de control.
	Alto	3	Riesgo alto requiere de la atención de la alta Gerencia, planes de tratamiento requeridos, implementados y reportados a las líneas de supervisión.
	Extremo	4	Riesgo Extremo se requiere de acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.
	Catastrófico	5	Cuando se produce está en riesgo la continuidad del negocio.

Elaborado por: Andrés Aguayo Yépez.

b) Complejidad de las operaciones e impacto en los procesos críticos de la organización.

Cuadro No. 13.

Factores de Riesgo	Nivel de Impacto	Valoración	Descripción del Nivel de Impacto
Complejidad de las operaciones e impacto en los procesos críticos de la organización.	Bajo	1	Riesgos que afectan superficialmente al proceso crítico y que pueden ser aceptados o fácilmente superables en el tiempo.
	Moderado	2	Cuando el subproceso no consta en el detalle de "Procesos Críticos de la Organización"
	Alto	3	Pérdida de eficiencia y calidad de ejecución en procesos críticos que generen riesgos por carga operativa adicional ocasionando: reproceso y recuperación de datos por errores.
	Extremo	4	Generen pérdida o fuga de información crítica, integridad y/o confiabilidad de información que es parte del core del negocio.
	Catastrófico	5	Cuando el subproceso consta en el detalle de "Procesos Críticos de la Organización"

Elaborado por: Andrés Aguayo Yépez.

c) Nivel de presión de la administración para el logro de objetivos estratégicos.

Cuadro No. 14.

Factores de Riesgo	Nivel de Impacto	Valoración	Descripción del Nivel de Impacto
Nivel de presión de la administración para el logro de objetivos estratégicos.	Bajo	1	Cuando el subproceso afecta de 0 a 2 objetivos estratégicos
	Moderado	2	Cuando el subproceso afecta de 3 a 4 objetivos estratégicos
	Alto	3	Cuando el subproceso afecta de 5 a 6 objetivos estratégicos
	Extremo	4	Cuando el subproceso afecta de 7 a 8 objetivos estratégicos
	Catastrófico	5	Cuando el subproceso afecta de 9 a más objetivos estratégicos

Elaborado por: Andrés Aguayo Yépez.

d) Resultado de auditorías independientes anteriores.

Cuadro No. 15.

Factores de Riesgo	Nivel de Impacto	Valoración	Descripción del Nivel de Impacto
Resultado de auditorías independientes anteriores	Bajo	1	Observaciones de forma
	Moderado	2	Incumplimiento de Procedimientos - Observaciones que afectan a la eficiencia y eficacia y que no necesariamente podría representar un impacto material
	Alto	3	Incumplimiento: Regulatorio y Política Interna que podría representar un impacto material significativo
	Extremo	4	Riesgo Reputacional - Perdida de recursos (dinero, datos, activos)
	Catastrófico	5	Afecta al negocio en marcha

Elaborado por: Andrés Aguayo Yépez.

e) Impacto en lavado de activos, exposición política y publicidad adversa.

Cuadro No. 16.

Factores de Riesgo	Nivel de Impacto	Valoración	Descripción del Nivel de Impacto
Impacto en lavado de activos,exposición política y publicidad adversa	Bajo	1	No contar con un procedimiento formal para la difusión interna de documentación recibida de organismos de control (Nacionales e Internacionales).
	Moderado	2	Cuando el subproceso "NO" consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos"
	Alto	3	Desconocimiento de leyes y regulaciones. No entrega de reportes requeridos por el organismo de control.
	Extremo	4	Observaciones de los organismos de control que ocasionen el deterioro de la calificación de la entidad Sanciones a accionistas o directores (destitución y multas).
	Catastrófico	5	Cuando el subproceso consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos"

Elaborado por: Andrés Aguayo Yépez.

f) Tiempo no auditado.

Cuadro No. 17.

Factores de Riesgo	Nivel de Impacto	Valoración	Descripción del Nivel de Impacto
Tiempo no auditado	Bajo	1	Si el subproceso fue evaluado en el período de 0 a 6 mes
	Moderado	2	Si el subproceso fue evaluado en el período de 7 a 12 mes
	Alto	3	Si el subproceso fue evaluado en el período de 13 a 19 mes
	Extremo	4	Si el subproceso fue evaluado en el período de 20 a 24 mes
	Catastrófico	5	Proceso no evaluado

Elaborado por: Andrés Aguayo Yépez.

PASO 3: PONDERACIÓN DE LOS FACTORES DE RIESGO:

Una vez efectuada la valoración de riesgo a cada subproceso para cada "factor de riesgo", se ha definido en este estudio el peso o porcentaje de ponderación que cada factor de riesgo tiene en base al criterio profesional, la experiencia y juicio del auditor. A continuación se presenta los porcentajes asignados:

Cuadro No. 18.

Factores de Riesgo	% de Ponderación
Calidad del sistema de control interno a través de la matriz de riesgos institucionales	30%
Complejidad de las operaciones e impacto en los procesos críticos de la organización.	20%
Nivel de presión de la administración para el logro de objetivos estratégicos.	18%
Impacto en lavado de activos, exposición política y publicidad adversa	12%
Resultado de auditorías independientes anteriores	15%
Tiempo no auditado	5%
TOTAL	**100%**

Elaborado por: Andrés Aguayo Yépez.

PASO 4: DETERMINAR EL NIVEL DE CRITICIDAD:

Para poder determinar el riesgo de cada subproceso una vez aplicados los criterios desarrollados en los pasos anteriores, se ha diseñado en

este estudio el “rango de criticidad” mismo que se presenta a continuación:

Cuadro No. 19.

RANGO DE CRITICIDAD		
-	1.00	BAJO
1.01	2.00	MODERADO
2.01	3.00	ALTO
3.01	4.00	EXTREMO
4.01	5.00	CATASTRÓFICO

Elaborado por: Andrés Aguayo Yépez.

Es decir, la calificación que obtenga cada subproceso una vez aplicado el porcentaje de ponderación referido en el cuadro No.18, nos dará como resultado un valor, el mismo que se lo homologará con el rango de “criticidad” arriba descrito cuadro No.19 y así se logra determinar el nivel de riesgo de cada subproceso.

IDENTIFICACIÓN DE PLANES DE TRATAMIENTO A LOS RIESGOS IDENTIFICADOS.

El paso posterior a la determinación del nivel de riesgo de los procesos de gestión tecnológica valorados a través de la adaptación metodológica, consiste en identificar las opciones procedimentales para mitigarlos, sin embargo desde el punto de vista de auditoría lo que se pretende es más bien auditarlos; con la finalidad de verificar el impacto

que estos procesos y subprocesos podrían tener de no ser controlados a través de un examen de aseguramiento (auditoria).

La determinación del nivel de riesgo de cada subproceso facilita y encamina los esfuerzos del departamento de auditoría hacia la revisión y el examen de áreas de riesgo por tanto la adaptación metodológica facilita tal misión, los pasos a considerar para llevar a cabo esta labor requieren:

Diseño del plan anual de auditoría:

El plan anual de auditoría será elaborado considerando lo siguiente: i) plan estratégico con enfoque de riesgos, ii) evaluación de controles internos y otros aspectos relacionados con riesgos, iii) revisión de la razonabilidad de los estados financieros, registro contables y otros aspectos, iv) cumplimiento legal, observaciones y recomendaciones de informes anteriores de auditoría interna y externa.

En lo referente a la evaluación de controles internos y otros aspectos relacionados con riesgos, deberá establecerse un enfoque especial para los procesos core (vitales) de la organización.

Una vez definido el enfoque sobre los procesos a revisar en el año, se define el alcance general asignando a los procesos, una estimación de personal y de tiempo. Esto se calcula en función de las horas-hombre disponibles considerando las horas realmente aplicadas en la ejecución

del plan anual, ya que no se debe considerar las horas de vacación ni aquellas invertidas en capacitación.

Diseñado y terminado el plan, debe ser puesto a consideración de la Administración para su conocimiento y aprobación. Posteriormente, el plan podría ser enviado a los distintos entes de control de ser necesario en las fechas por ellos establecidos. El plan deberá ser reformulado en el caso de que exista un evento/ riesgo/oportunidad que requiera una inversión de horas no prevista.

Diseñar programas de trabajo:

Los auditores deben elaborar programas de trabajo, cuyo contenido esté encaminado a cumplir con los siguientes objetivos:

Asegurar la confiabilidad e integridad de la información a ser analizada: los auditores deben revisar información financiera y operativa, y los medios usados para identificar, medir, clasificar y reportar dicha información; deben examinar los sistemas de información y de control interno para cerciorarse de que: i) contienen información exacta, ii) confiable, oportuna y útil, iii) los procedimientos imperantes en el ciclo que permiten generar la información se están ejecutando de la forma prevista por la Administración, iv) los controles para la generación son adecuados y efectivos, v) los riesgos imperantes en los diferentes ciclos del negocio, están siendo medidos, monitoreados y controlados.

Verificar el cumplimiento con políticas, procedimientos, leyes y normas y prácticas autorizadas: los auditores deben evaluar si las políticas y procedimientos establecidos por la Administración, se cumplen y si están en línea con las leyes, normas y prácticas definidas por los organismos de control y las mejores prácticas aplicables sobre todo en cuanto a los riesgos identificados como por ejemplo: i) verificar el resguardo de activos, ii) verificar el empleo eficiente de los recursos, iii) verificar el cumplimiento de los objetivos y metas establecidas para operaciones o programas:

Los programas de trabajo deben definir los tipos de pruebas a ejecutarse en la auditoria

El auditor deberá seleccionar la prueba que más se ajuste al objetivo de auditoría que se persigue a través de: i) pruebas detalladas de transacciones y saldos, ii) procedimientos analíticos, iii) pruebas de control.

El propósito fundamental en la etapa de ejecución es recopilar las pruebas que sustenten las opiniones del auditor en cuanto al trabajo realizado, esta depende sustancialmente del grado de profundidad con que se haya trabajado en la etapa anterior (planificación), en esta etapa se elaboran los papeles de trabajo y el sustento del trabajo desarrollado. Durante el proceso de ejecución, los auditores deberán: i) recolectar información relacionada con las actividades a auditar, ii) aplicar los programas de trabajo previamente diseñados y aprobados, iii) identificar

hallazgos u observaciones, iv) obtener evidencia de auditoría; y, v) supervisar y obtener evidencia de supervisión del trabajo realizado y definir si los procedimientos de auditoría deben o no ser modificados de acuerdo a la importancia y significatividad de las circunstancias.

Los auditores en todo tiempo deben comunicar de manera oportuna al Auditor General y/o Líder del equipo de trabajo sobre los resultados del trabajo en proceso, así como de las limitaciones o aspectos que impidan completar las tareas programadas en el tiempo definido para tomar las acciones pertinentes.

Al momento de identificar un hallazgo y haber obtenido evidencia del mismo deberán indagar con el auditado la causa del mismo con el objeto de formular una recomendación que mitigue de raíz el efecto de esa práctica. Así mismo, el auditor deberá indagar si el efecto del hallazgo tiene más implicancias en otros procesos o en efectos monetarios/contables con el fin de determinar si aplica la cuantificación de un efecto para sugerir el auditado su corrección, adicional se deberá documentar todo su trabajo (papeles de trabajo).

Por lo tanto todas las etapas de auditoría: planificación, ejecución y emisión de informes tienen que ser documentadas y deberán contener como mínimo:

- Permite un registro ordenado del trabajo desempeñado y de las conclusiones.

- Permite que el equipo de auditoría a adoptar una disciplina y un consistente enfoque en su trabajo.

- Facilita la revisión del senior y gerente de auditoría, y provee evidencia de esa revisión.

- Salva los programas de auditoría como base para futuros trabajos.

- Facilita el uso de formatos estandarizados.

- Facilita la capacidad para salvar información, experiencia y trabajo de una auditoría para las siguientes revisiones futuras.

- Trabaja en ambiente windows, permitiendo incluir documentos de: word/excel/power point/ imágenes escaneadas, etc. como papeles de trabajo con sus correspondientes referencias cruzadas.

- Permite ordenar el plan por procedimiento o por área auditada.

- Categoriza las tareas y hallazgos en: no iniciado, en progreso, terminado y revisado.

- La información se puede obtener por diferentes “vistas” de: procedimientos, hallazgos, notas a ser aclaradas, y estatus de avance de todos los documentos.

- Permite administrar varios proyectos por separado: plan de auditoría, requerimientos especiales, etc.

- Permite la interrelación entre: área auditada, detalles de la prueba (objetivo, alcance, instrucciones), trabajo realizado, conclusión, evidencia de quien y cuando ejecutó y revisó, estatus de la prueba, referencia y evidencia del trabajo.

- Referencia a hallazgos (red flags) detectados.

- Permite la creación de informes inmediatos, pues clasifica los hallazgos: tipo (estrategia, procesos, organización, tecnología) categoría (riesgo alto, riesgo medio, riesgo bajo) niveles (eficiencia y/o eficacia, cumplimiento, alineación con capacidades)

6.3. MEDICION Y PRESENTACIÓN DEL NIVEL DE RIESGO OBTENIDO.

CASO DE APLICACIÓN (3era parte – construcción de la matriz de riesgo operacional)

Todos aquellos procesos y subprocesos de gestión tecnológica determinados como vulnerables y por tanto que tienen riesgo operativo

ahora pasan a una matriz de riesgo en donde aplicando el instructivo propuesto y desarrollado en esta investigación dan como resultado una calificación de riesgo asignado a cada subproceso, estos resultados se presentan de manera amplia y detallada en el **Anexo No. 2.**

CRITERIOS DE CUANTIFICACIÒN DE PÉRDIDAS MONETARIAS POR RIESGO.

Con la finalidad cuantificar, en términos monetarios, las posibles pérdidas en las que incurriría una organización debido a riesgo operativo, es necesario mencionar dos metodologías sugeridas para el efecto[23]:

- Metodologías estadísticas, y ;
- Metodologías causales.

METODOLOGIAS ESTADÍSTICAS:

Esta metodología se basa en la información histórica sobre las variables relevantes, y son el criterio más coherente para la determinación de la pérdida por riesgo operativo ya que evita la subjetividad, ejemplos:

- CAPM – Capital Asset Pricing Model.
- Mapa de riesgos.
- Value at Risk (VaR) - Cash Flow at Risk.
- Modelos de Regresión.

[23] UNIVERSIDAD DE LOS ANDES, A. Mendoza & M. Castillo. “Diseño de una metodología para la identificación del riego operativo en instituciones financieras” Bogotá-Colombia.

- Análisis discriminante – Regresión logística.

CAPM – Capital Asset Pricing Model.

Este es un modelo de valoración de activos financieros, ampliamente utilizado con la finalidad de determinar la tasa de retorno (TIR) para un activo, consideramos que este modelo no es aplicable para determinar la pérdida por riesgo operativo en tecnologías de la información.

Mapa de riesgos.

Implica la identificación del lugar generador de riesgo, diagramar los procesos y subprocesos, y ubicar los riesgos en tales procesos, para después categorizarlos usando las variables impacto-probabilidad, revisa la efectividad de controles y determina un riesgo residual, este metodología es a nuestro criterio la más apropiada para este estudio.

Value at Risk (VaR) - Cash Flow at Risk.

Es una medida del riesgo de tipo estadístico, pero requiere para su ejecución de información histórica, normalmente se usa para medir el riesgo de una cartera de créditos en una institución financiera, por la carencia de información histórica relacionada con las tecnologías de información no es aplicable.

Modelos de Regresión.

Requiere no solo de información y data histórica sino que además es necesario la adquisición y utilización de un software para la construcción de un modelo de regresión que utilice variables que expliquen el modelo, por la falta de información histórica no es la mejor alternativa para la investigación planteada.

Análisis discriminante – Regresión logística.

Se basa en la técnica de separar objetos u observaciones a grupos previamente definidos, planteo estadístico que a partir de una muestra de entrenamiento, es decir, un conjunto de objetos cuya pertenencia a uno de los grupos preestablecidos se conoce, se deriva una regla que permite asignar cada una de las observaciones a uno de los grupos mutuamente excluyentes, minimizando la probabilidad de clasificar incorrectamente a los individuos, no aplicable al presente estudio.

METODOLOGIAS CAUSALES:

Se basan en los juicios de expertos con la posibilidad de tener en cuenta la información histórica, y al basarse en juicios caen en el campo de la subjetividad por tanto consideramos que para los fines de este trabajo de investigación no es relevante, los siguientes son los ejemplos de esta metodología:

- Redes Bayesianas.
- Distribución de influencia.

- Simulación de montecarlo.

6.4. PRESENTACION DE RESULTADOS OBTENIDOS.

Una vez determinado el nivel de riesgo asignado a los subprocesos evaluados (anexo No.2), utilizando como impacto los niveles de calificación del riesgo determinados (bajo, moderado, alto, extremo y catastrófico) y como probabilidad la ponderación asignada a los factores de riesgo determinados bajo el criterio y juicio profesional de auditoría interna (calidad del sistema de control interno a través de la matriz de riesgos institucionales; complejidad de las operaciones e impacto en los procesos críticos de la organización; nivel de presión de la administración para el logro de objetivos estratégicos; impacto en lavado de activos, exposición política y publicidad adversa; resultado de auditorías independientes anteriores; y tiempo no auditado) los resultados por proceso se presentan así:

Cuadro No. 20.

Administración de infraestructura:

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	5
EXTREMO	4
CATASTRÓFICO	0
TOTAL	9

Los procesos evaluados en la gestión tecnológica de administración de infraestructura, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en riesgos muestra que: del 100% de los procesos

valorados el 55% de los procesos tiene riesgo de alto impacto mientras que el 45% de los procesos tienen riesgo de extremo impacto.

Cuadro No. 21.

Desarrollo, mantenimiento e implementación de software:

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	5
EXTREMO	1
CATASTRÓFICO	0
TOTAL	6

Los procesos evaluados en la gestión tecnológica de desarrollo, mantenimiento e implementación de software, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en riesgos muestra que: del 100% de los procesos valorados el 83% de los procesos tiene riesgo de alto impacto mientras que el 17% de los procesos tienen riesgo de extremo impacto

Cuadro No. 22.

Gestión de seguridad de información:

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	3
EXTREMO	1
CATASTRÓFICO	0
TOTAL	4

Los procesos evaluados en la gestión tecnológica de gestión de seguridad de la información, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en riesgos muestra que: del 100% de los

procesos valorados el 75% de los procesos tiene riesgo de alto impacto mientras que el 25% de los procesos tienen riesgo de extremo impacto.

Cuadro No. 23.

Gestión de soporte a usuarios:

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	1
ALTO	5
EXTREMO	4
CATASTRÓFICO	0
TOTAL	10

Los procesos evaluados en la gestión tecnológica de gestión de soporte a usuarios, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en riesgos muestra que: del 100% de los procesos valorados el 10% de los procesos tiene riesgo de moderado impacto, el 50% de los procesos tiene riesgo de alto impacto, mientras que el 40% de los procesos tienen riesgo de extremo impacto.

Cuadro No. 24.

Monitoreo de sistemas y aplicaciones y procesamiento tecnológico:

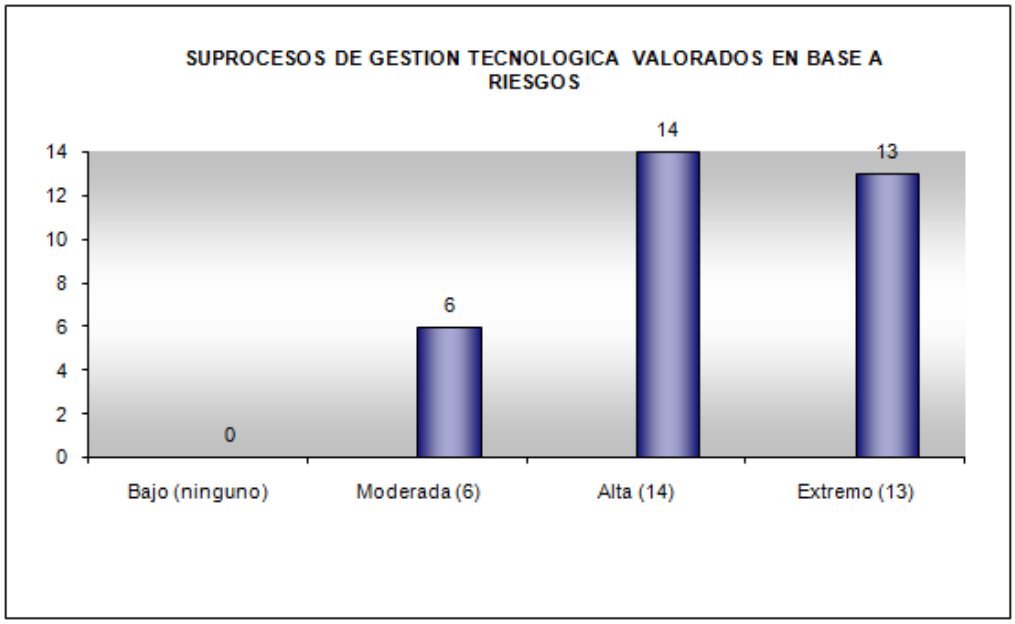
CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	1
EXTREMO	3
CATASTRÓFICO	0
TOTAL	4

Los procesos evaluados en la gestión tecnológica de monitoreo de sistemas y aplicaciones y procesamiento tecnológico, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en

riesgos muestra que: del 100% de los procesos valorados el 25% de los procesos tiene riesgo de alto impacto mientras que el 75% de los procesos tienen riesgo de extremo impacto.

Subprocesos de gestión tecnológica medidos en función a los factores de riesgo determinados metodológicamente:

Gráfico No. 10.



Elaborado por: Andrés Aguayo Yépez.

Los procesos evaluados en la gestión tecnológica, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en riesgos muestra que: del 100% de los procesos valorados el 18% de los procesos tiene riesgo de moderado impacto, el 42% de los procesos tiene riesgo de alto impacto, mientras que el 40% de los procesos tienen riesgo de extremo impacto. Esta información nos permite identificar el

nivel de riesgo que tienen los procesos antes descritos de manera cualitativa, más por el alcance del presente estudio no pretende valorar el nivel financiero y económico de pérdidas asignadas por riesgo.

Subprocesos de gestión tecnológica diagramados en la matriz de riegos:

Gráfico No. 11.

MATRIZ DE RIESGOS

		1	2	3	4	5
	Probab/Impacto	Bajo	Moderado	Alto	Extremo	Catastrófico
5	Casi Certera			Gestión de seguridad de información	Gestión de seguridad de información	
4	Probable		Gestión de soporte a usuarios	Administración de infraestructura	Administración de infraestructura	
3	Posible			Desarrollo, mantenimiento e implementación de software	Desarrollo, mantenimiento e implementación de software	
2	Improbable			Monitoreo de sistemas y aplicaciones y procesamiento tecnológico	Monitoreo de sistemas y aplicaciones y procesamiento tecnológico	
1	Rara					

Elaborado por: Andrés Aguayo Yépez.

Los procesos de gestión tecnológica, valorados cualitativamente a través de la adaptación metodológica para la medición del riesgo operativo con enfoque de auditoría basado en riesgos muestra que sus subprocesos tienen nivel de riesgo que va desde: nivel moderado para la proceso de gestión de soporte a usuarios, nivel alto y extremo para los procesos de gestión de seguridad de información; administración de la infraestructura; desarrollo, mantenimiento e implementación de software; y, monitoreo de sistemas y procesamiento tecnológico.

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES.

El presente trabajo de investigación (adaptación metodológica) ha permitido verificar a través del desarrollo tanto conceptual como práctico a razón de sus dos matrices tanto la de identificación de procesos y subprocesos vulnerables (anexo No.1) y la matriz de riesgos valorados en función de factores de riesgo (anexo No.2) que cumple efectivamente en su construcción y desarrollo con las mejores prácticas de gestión de riesgos, inclusive considero mencionar que bajo el esquema planteado cumple adicionalmente con el marco de referencia internacional para la práctica y el ejercicio de la auditoría interna.

Este ambiente de evolución permanente, determinado por las actuales tendencias mundiales, las cuales se centran en el plano económico soportadas por la evolución tecnológica, incrementan en todo tiempo la necesidad de que la función de auditoría interna requiera constante y

continuamente el mejoramiento de su gestión y con el desarrollo de esta investigación ha quedado evidencia de ello.

Este esquema de identificación de procesos vulnerables para las tecnologías de información ha brindado un primer paso para sobre la base de esta experiencia valorar más procesos y subprocesos en este campo y ampliar la conceptualización del riesgo, pero no solo llegando hasta este nivel, ya que el estudio ha logrado generar la determinación de un nivel de riesgo de cada subproceso, el mismo que es útil como primer insumo hacia una determinación de entes a ser auditados en función prioritaria a su nivel de riesgo, por tanto este esquema planteado genera valor agregado al momento de prepararse un plan anual del trabajo de auditoría.

Este estudio ha procurado deslindarse de la subjetividad y más bien apoyarse en la fundamentación teórica agregando el criterio y el juicio profesional de un auditor, sin embargo para que esta nueva metodología funcione se necesita un cambio radical en la cultura y en los esquemas de control en las organizaciones mismo que deberá estar soportado por la decisión de los más altos niveles directivos de la organización.

En este ámbito de transformación de la auditoría interna, los sistemas informáticos de la organización representan un reto y una solución cuando son utilizados como un medio de evaluación constante de controles. A través de las técnicas para la evaluación de operaciones

procesadas a través de sistemas informáticos se podrá desarrollar un sistema automatizado de revisión, el cual permitirá a la auditoría cambiar de un enfoque de revisión periódica a un enfoque de revisión constante y bajo un ambiente de riesgo.

Es necesario recalcar que la presente investigación ha sido efectuada con el apoyo de personal experto y conocedor de las tecnologías de información, quienes en base a su criterio profesional han orientado los esfuerzos de la investigación a objetivos reales, que son la base para en lo posterior desarrollar un esquema de valoración cuantitativa de riesgo operacional que permita evaluar el impacto financiero de los distintos procesos y subprocesos en los estados financieros tomados en conjunto, de igual manera es importante mencionar que este estudio está ligado a los riesgos asociados al sector bancario y específicamente a las instituciones financieras, que sin excluir su aplicabilidad metodológica a otras industrias son funcionalmente aplicables al sector financiero como primer filtro.

7.2. RECOMENDACIONES.

Esta investigación pretende determinar un nivel de riesgo por subproceso basada en las mejores prácticas disponibles en el medio, de tal forma de tener un mecanismo de determinación de riesgo de manera cualitativa de primera instancia, sin embargo es recomendable que en un estudio posterior se desarrolle un mecanismo propio de valoración cuantitativa del riesgo que permita pasar del análisis cualitativo a un cuantitativo que determine un nivel de pérdida estimado a un proceso determinado.

La adaptación de este marco metodológico está soportado en modelos conceptuales, y sus pasos han sido argumentados durante el desarrollo del presente estudio, no sólo identifica las principales fuentes de riesgo operativo en las tecnologías de información, sino también valora de manera cualitativa el nivel de exposición al riesgo valorado en función de factores de riesgo determinados con juicio profesional de auditoría.

El estudio no pretende calcular las provisiones que deben realizar las entidades financieras para cubrir eventos de pérdida ya que el acceso a la información que permite calcular tales requerimientos de provisión son limitados y los modelos pro babilísticos que soportan tal calculo lo requieren como condición sine qua non.

El proceso de recolección de la información, tanto cualitativa como cuantitativa, es de particular importancia para la aplicación de la metodología antes referida.

Finalmente considero que es necesario para las entidades financieras ecuatorianas orientar sus esfuerzos hacia la construcción de una base de datos organizada con información sobre los eventos de pérdida que se vayan presentando. Esto permitirá obtener resultados más precisos al aplicar una metodología integral de valoración de riesgos que considere aspectos cualitativos como cuantitativos en el futuro inmediato.

7.3. BIBLIOGRAFIA.

- LIBRO DE REGLAS DE INTERNATIONAL BANKING

- SANAS PRACTICAS PARA LA ADMINISTRACION Y SUPERVISION DEL RIESGO OPERACIONAL, Comité de Basilea sobre supervisión bancaria.

- LEY GENERAL DE INSTRUCCIONES DEL SISTEMA FINANCIERO, REGLAMENTO - RESOLUCIONES. ACTUALIZADO A FEBRERO DE 2010.

- Asociación de Auditoría y Control de Sistemas de Información (ISACA, en inglés) www.isaca.org

- Instituto de Auditores Internos (IIA, en inglés) – www.theiia.org

- Kevin Behr, Gene Kim, George Spafford, The Visible Ops Handbook: Starting ITIL In 4 Practical Steps, IT Process Institute, 2004.

- Jennifer Bayuk, Productive Intrusion Detection, Computer Security Journal, Volume XVIII, 3-4, 2002, págs. 23 a 33.

- Peter Mell, Tiffany Bergeron, David Henning, Creating a Patch and Vulnerability Management Program, Special Publication 800-40 v2.0, NIST, 2005.

- Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad (editors), Security Patterns: Integrating Security and Systems Engineering, Wiley & Sons, 2006.

- Jay R. Taylor, Julia Allen, Glenn Hyatt, Gene Kim, Controles de gestión de parches y cambios: cruciales para el éxito de la organización, The IIA, 2005.

- Gary Stoneburner, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems, Special Publication 800-30, NIST 2002.

- Grupo de Trabajo de Seguridad de la Información Corporativa, Report of the Best Practices and Metrics Teams, Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés)

- Oficina de Comercio de Gobierno, IT Infrastructure Library, www.itil.co.uk.

7.4. ANEXOS

ANEXO No. 1 (a)

Macroproceso	Proceso	Subprocesos	Se encuentra dentro de los dominios COBIT?		PARAMETROS DE DETECCION DE VULNERABILIDADES								
			SI	NO	Tipo de Dominio COBIT	Tipo de recurso según COBIT	Cantidad de incidentes al año 2010	Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.	Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.	Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.	Falta de un sistema de gestión de activos.	Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades.	Subproceso es vulnerable?
Gestión de Tecnología	Administración de Infraestructura	Administración y monitoreo de accesos remotos	X		(PO)	Infraestructura	26.209	SI	NO	NO	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Administración y monitoreo de equipos de la red WAN y equipos de comunicaciones	X		(PO)	Infraestructura	2.884	NO	NO	NO	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Administración, monitoreo y diseño de funcionamiento de servidores para revisión de logs	X		(PO)	Infraestructura	1.131	NO	SI	NO	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Compactación de bases correo electrónico	X		(PO)	Infraestructura	6.555	NO	SI	NO	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Diseño de soluciones de comunicaciones	X		(PO)	Infraestructura	342	SI	SI	SI	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Disponibilidad de memoria RAM	X		(PO)	Infraestructura	634	SI	NO	NO	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Disponibilidad de procesador	X		(PO)	Infraestructura	400	NO	SI	NO	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Monitoreo y administración de centrales telefónicas	X		(PO)	Infraestructura	802	NO	SI	SI	NO	SI	SI
Gestión de Tecnología	Administración de Infraestructura	Revisión de espacio disponible y de uso de los discos duros	X		(PO)	Infraestructura	20.447	SI	SI	NO	NO	SI	SI

(PO)	Planear y Organizar

Fuente: THE INSTITUTE OF INTERNAL AUDITORS (IAI)

Elaborado por: Andrés Aguayo Yépez.

ANEXO No. 1 (b)

Macroproceso	Proceso	Subprocesos	Se encuentra dentro de los dominios COBIT?		PARAMETROS DE DETECCION DE VULNERABILIDADES								
			SI	NO	Tipo de Dominio COBIT	Tipo de recurso según COBIT	Cantidad de incidentes al año 2010	Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.	Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.	Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.	Falta de un sistema de gestión de activos.	Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades.	Subproceso es vulnerable?
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Atención de requerimientos de tecnología	X		(DS)	Aplicaciones	2208	NO	NO	NO	NO	SI	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de facturación	X		(DS)	Aplicaciones	138	SI	SI	NO	NO	SI	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de ambientes	X		(DS)	Aplicaciones	56	SI	NO	NO	SI	SI	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Pruebas técnicas y de certificación	X		(DS)	Aplicaciones	5897	SI	SI	SI	NO	SI	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a producción	X		(DS)	Aplicaciones	8542	SI	SI	NO	NO	SI	SI
Gestión de Tecnología	Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a pruebas	X		(DS)	Aplicaciones	6339	NO	SI	NO	NO	NO	SI

(DS)	Entregar y Dar Soporte

Fuente: THE INSTITUTE OF INTERNAL AUDITORS (IAI)

Elaborado por: Andrés Aguayo Yépez.

ANEXO No. 1 (c)

Macroproceso	Proceso	Subprocesos	Se encuentra dentro de los dominios COBIT?		PARAMETROS DE DETECCION DE VULNERABILIDADES								
			SI	NO	Tipo de Dominio COBIT	Tipo de recurso según COBIT	Cantidad de incidentes al año 2010	Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.	Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.	Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.	Falta de un sistema de gestión de activos.	Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades.	Subproceso es vulnerable?
Gestión de Tecnología	Gestión de Seguridad de Información	Administración de usuarios	X		(ME)	Personas	12.127	SI	SI	SI	NO	SI	SI
Gestión de Tecnología	Gestión de Seguridad de Información	Administración y autenticación de backups internos y externos	X		(ME)	Personas	33	NO	SI	NO	NO	SI	SI
Gestión de Tecnología	Gestión de Seguridad de Información	Procedimiento de control de cambios	X		(ME)	Personas	1.000	NO	NO	SI	SI	SI	SI
Gestión de Tecnología	Gestión de Seguridad de Información	Procedimiento para reprocesos	X		(ME)	Personas	1.497	SI	SI	SI	SI	SI	SI

(ME)	Monitorear y Evaluar

Fuente: THE INSTITUTE OF INTERNAL AUDITORS (IAI)

Elaborado por: Andrés Aguayo Yépez.

ANEXO No. 1 (d)

Macroproceso	Proceso	Subprocesos	Se encuentra dentro de los dominios COBIT?		PARAMETROS DE DETECCION DE VULNERABILIDADES								
			SI	NO	Tipo de Dominio COBIT	Tipo de recurso según COBIT	Cantidad de incidentes al año 2010	Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.	Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.	Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.	Falta de un sistema de gestión de activos.	Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades.	Subproceso es vulnerable?
Gestión de Tecnología	Gestión Soporte a Usuarios	Atención de requerimientos	X		(AI)	Personas	5.984	NO	SI	SI	NO	SI	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Atención helpdesk	X		(AI)	Personas	3.826	NO	SI	SI	SI	NO	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Atención requerimientos WEB	X		(AI)	Personas	2.754	SI	SI	SI	NO	SI	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Creación de usuarios de correo electrónico	X		(AI)	Personas	2.049	NO	SI	SI	SI	SI	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Eliminación de usuarios de correo electrónico	X		(AI)	Personas	91	NO	SI	NO	SI	SI	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Entrega de reportes por requerimiento de usuario	X		(AI)	Personas	8.105	SI	NO	SI	NO	SI	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Generación de informes	X		(AI)	Personas	20.447	SI	NO	SI	SI	NO	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Preparación de equipos	X		(AI)	Personas	1.879	NO	SI	SI	SI	NO	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Revisión de actualización del sistema operativo	X		(AI)	Personas	3.826	SI	SI	NO	SI	SI	SI
Gestión de Tecnología	Gestión Soporte a Usuarios	Revisión de definiciones antivirus	X		(AI)	Personas	3.008	NO	SI	NO	SI	SI	SI

(AI)	Adquirir e Implementar

Fuente: THE INSTITUTE OF INTERNAL AUDITORS (IAI
Elaborado por: Andrés Aguayo Yépez.

ANEXO No. 1 (e)

Macroproceso	Proceso	Subprocesos	Se encuentra dentro de los dominios COBIT?		PARAMETROS DE DETECCION DE VULNERABILIDADES								
			SI	NO	Tipo de Dominio COBIT	Tipo de recurso según COBIT	Cantidad de incidentes al año 2010	Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.	Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.	Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.	Falta de un sistema de gestión de activos.	Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades.	Subproceso es vulnerable?
Gestión de Tecnología	Monitoreo de Sistemas y Aplicaciones	Monitoreo de servicios, sistemas y aplicaciones	X		(DS)	Aplicaciones	610	SI	SI	NO	NO	SI	SI
Gestión de Tecnología	Procesamiento Tecnológico	Parametrizaciones	X		(ME)	Información	61.436	SI	SI	NO	NO	SI	SI
Gestión de Tecnología	Procesamiento Tecnológico	Procesamiento de transacciones y disponibilidad de información	X		(ME)	Información	573	SI	SI	SI	NO	SI	SI
Gestión de Tecnología	Procesamiento Tecnológico	Seguimiento y paso a producción	X		(ME)	Información	1.979	SI	SI	SI	SI	SI	SI

(DS)	Entregar y Dar Soporte
(ME)	Monitorear y Evaluar

Fuente: THE INSTITUTE OF INTERNAL AUDITORS (IAI)

Elaborado por: Andrés Aguayo Yépez.

ANEXO No. 2 (a)

PROCESO	FLUJOGRAMA	CALIDAD DEL SISTEMA DE CONTROL INTERNO A TRAVES DE LA MATRIZ DE RIESGOS INSTITUCIONALES: BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
		Menores efectos que pueden ser facilmente remediados. Si el riesgo es bajo se administra con procedimientos rutinarios, si es insignificante no requiere ninguna acción.	Riesgo moderado y aceptable debe ser administrado con procedimientos normales de control.	Riesgo alto requiere de la atención de la alta Gerencia, planes de tratamiento requeridos, implementados y reportados a las líneas de supervisión	Riesgo Extremo se requiere de acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.	Cuando se produce está en riesgo la continuidad del negocio.
Administración de Infraestructura	Administración y monitoreo de accesos remotos			3		
Administración de Infraestructura	Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones		2			
Administración de Infraestructura	Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs			3		
Administración de Infraestructura	Compactación de Bases Correo Electrónico	1				
Administración de Infraestructura	Diseño de soluciones de comunicaciones	1				
Administración de Infraestructura	Disponibilidad de Memoria RAM				4	
Administración de Infraestructura	Disponibilidad de Procesador			3		
Administración de Infraestructura	Monitoreo y administración de centrales telefónicas			3		
Administración de Infraestructura	Revisión de Espacio disponible y de uso de los Discos Duros		2			

FLUJOGRAMA	COMPLEJIDAD DE LAS OPERACIONES E IMPACTO EN LOS PROCESOS CRITICOS DE LA ORGANIZACIÓN: BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	Riesgos que afectan superficialmente al proceso crítico y que pueden ser aceptados o facilmente superables en el tiempo.	Cuando el subproceso no consta en el detalle de "Procesos Críticos de la Organización"	Pérdida de eficiencia y calidad de ejecución en procesos críticos que generen riesgos por carga operativa adicional ocasionando: reprocesos y recuperación de datos por errores.	- Generen pérdida o fuga de información crítica, integridad y/o confiabilidad de información que es parte del core del negocio.	Cuando el subproceso consta en el detalle de "Procesos Críticos de la Organización"
Administración y monitoreo de accesos remotos				4	
Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones					5
Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs					5
Compactación de Bases Correo Electrónico				4	
Diseño de soluciones de comunicaciones				4	
Disponibilidad de Memoria RAM					5
Disponibilidad de Procesador					5
Monitoreo y administración de centrales telefónicas					5
Revisión de Espacio disponible y de uso de los Discos Duros				4	

FLUJOGRAMA	NIVEL DE PRESION DE LA ADMINISTRACION PARA EL LOGRO DE OBJETIVOS ESTRATEGICOS: BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	Cuando el subproceso afecta de 0 a 2 objetivos estratégicos	Moderado 2 Cuando el subproceso afecta de 3 a 4 objetivos estratégicos	Cuando el subproceso afecta de 5 a 6 objetivos estratégicos	Cuando el subproceso afecta de 7 a 8 objetivos estratégicos	Cuando el subproceso afecta de 9 a más objetivos estratégicos
Administración y monitoreo de accesos remotos				4	
Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones		2			
Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs		2			
Compactación de Bases Correo Electrónico		2			
Diseño de soluciones de comunicaciones		2			
Disponibilidad de Memoria RAM		2			
Disponibilidad de Procesador				4	
Monitoreo y administración de centrales telefónicas		2			
Revisión de Espacio disponible y de uso de los Discos Duros				4	

FLUJOGRAMA	IMPACTO EN LAVADO DE ACTIVOS, EXPOSICION POLITICA Y PUBLICIDAD ADVERSA: BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	No contar con un procedimiento forma para la difusión interna de documentación recibida de organismos de control (Nacionales e Internacionales).	Cuando el subproceso "NO" consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos"	- Desconocimiento de leyes y regulaciones. - No entrega de reportes requeridos por el organismo de control.	- Observaciones de los organismos de control que ocasionen el deterioro de la calificación de la entidad - Sanciones a accionistas o directores (destitución y multas).	Cuando el subproceso consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos" - Retiro de la franquicia.
Administración y monitoreo de accesos remotos				4	
Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones				4	
Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs				4	
Compactación de Bases Correo Electrónico		2			
Diseño de soluciones de comunicaciones				4	
Disponibilidad de Memoria RAM			3		
Disponibilidad de Procesador				4	
Monitoreo y administración de centrales telefónicas		2			
Revisión de Espacio disponible y de uso de los Discos Duros		2			

FLUJOGRAMA	RESULTADO DE AUDITORIAS INDEPENDIENTES ANTERIORES: BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	Informe limpio - Observaciones de Forma	Incumplimiento de Políticas y Procedimientos que afecten a la eficiencia y eficacia de los procesos/subprocesos. Proceso que no necesariamente debía ser evaluado en el ultimo año.	Incumplimiento regulatorio y de Política Interna	- Riesgo Reputacional - Existencia de un fraude. - Multas, sanciones que afecte a la calificación.	Observaciones determinadas afectan al negocio en marcha
Administración y monitoreo de accesos remotos			3		
Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones			3		
Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs		2			
Compactación de Bases Correo Electrónico		2			
Diseño de soluciones de comunicaciones			3		
Disponibilidad de Memoria RAM			3		
Disponibilidad de Procesador			3		
Monitoreo y administración de centrales telefónicas		2			
Revisión de Espacio disponible y de uso de los Discos Duros		2			

FLUJOGRAMA	TIEMPO NO AUDITADO: BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	Si el subproceso fue evaluado en el período de 0 a 6 meses	Si el subproceso fue evaluado en el período de 7 a 12 meses	Si el subproceso fue evaluado en el período de 13 a 19 meses	Si el subproceso fue evaluado en el período de 20 a 24 mes	Proceso no evaluado
Administración y monitoreo de accesos remotos	1				
Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones		2			
Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs	1				
Compactación de Bases Correo Electrónico		2			
Diseño de soluciones de comunicaciones		2			
Disponibilidad de Memoria RAM		2			
Disponibilidad de Procesador		2			
Monitoreo y administración de centrales telefónicas		2			
Revisión de Espacio disponible y de uso de los Discos Duros		2			

FLUJOGRAMA	30% FACTOR RO-1	20% FACTOR RO-2	18% FACTOR RO-3	12% FACTOR RO-4	15% FACTOR RO-5	5% FACTOR RO-6	PROMEDIO
Administración y monitoreo de accesos remotos	3	4	4	4	3	1	3,40
Administración y Monitoreo de Equipos de la Red WAN y Equipos de Comunicaciones	2	5	2	4	3	2	2,99
Administración, monitoreo y diseño de funcionamiento de servidores para Revisión de Logs	3	5	2	4	2	1	3,09
Compactación de Bases Correo Electrónico	1	4	2	2	2	2	2,10
Diseño de soluciones de comunicaciones	1	4	2	4	3	2	2,49
Disponibilidad de Memoria RAM	4	5	2	3	3	2	3,47
Disponibilidad de Procesador	3	5	4	4	3	2	3,65
Monitoreo y administración de centrales telefónicas	3	5	2	2	2	2	2,90
Revisión de Espacio disponible y de uso de los Discos Duros	2	5	4	2	2	2	2,96

Elaborado por: Andrés Aguayo Yépez.

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	5
EXTREMO	4
CATASTRÓFICO	0
TOTAL	**9**

ANEXO No. 2 (b)

PROCESO	FLUJOGRAMA	CALIDAD DEL SISTEMA DE CONTROL INTERNO A TRAVES DE LA MATRIZ DE RIESGOS INSTITUCIONALES					COMPLEJIDAD DE LAS OPERACIONES E IMPACTO EN LOS PROCESOS CRITICOS DE LA ORGANIZACIÓN				
		BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
		Menores efectos que pueden ser facilmente remediados. Si el riesgo es bajo se administra con procedimientos rutinarios, si es insignificante no requiere ninguna acción.	Riesgo moderado y aceptable debe ser administrado con procedimientos normales de control.	Riesgo alto requiere de la atención de la alta Gerencia, planes de tratamiento requeridos, implementados y reportados a las líneas de supervisión.	Riesgo Extremo se requiere de acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.	Cuando se produce está en riesgo la continuidad del negocio.	Riesgos que afectan superficialmente al proceso crítico y que pueden ser aceptados o facilmente superables en el tiempo.	Cuando el subproceso no consta en el detalle de "Procesos Críticos de la Organización"	Pérdida de eficiencia y calidad de ejecución en procesos críticos que generen riesgos por carga operativa adicional ocasionando: reprocesos y recuperación de datos por errores.	- Generen pérdida o fuga de información crítica, integridad y/o confiabilidad de información que es parte del core del negocio.	Cuando el subproceso consta en el detalle de "Procesos Críticos de la Organización"
Desarrollo, mantenimiento e implementación de software	Atención de requerimientos de tecnología			3						4	
Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de facturación	1								4	
Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de ambientes	1								4	
Desarrollo, mantenimiento e implementación de software	Pruebas técnicas y de certificación		2						3		
Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a producción		2							4	
Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a pruebas		2						3		

PROCESO	FLUJOGRAMA	NIVEL DE PRESION DE LA ADMINISTRACION PARA EL LOGRO DE OBJETIVOS ESTRATEGICOS					IMPACTO EN LAVADO DE ACTIVOS, EXPOSICION POLITICA Y PUBLICIDAD ADVERSA				
		BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
		Cuando el subproceso afecta de 0 a 2 objetivos estratégicos	Moderado 2 Cuando el subproceso afecta de 3 a 4 objetivos estratégicos	Cuando el subproceso afecta de 5 a 6 objetivos estratégicos	Cuando el subproceso afecta de 7 a 8 objetivos estratégicos	Cuando el subproceso afecta de 9 a más objetivos estratégicos	No contar con un procedimiento formal para la difusión interna de documentación recibida de organismos de control (Nacionales e Internacionales).	Cuando el subproceso "NO" consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos"	- Desconocimiento de leyes y regulaciones. - No entrega de reportes requeridos por el organismo de control.	- Observaciones de los organismos de control que ocasionen el deterioro de la calificación de la entidad - Sanciones a accionistas o directores (destitución y multas).	Cuando el subproceso consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos" - Retiro de la franquicia.
Desarrollo, mantenimiento e implementación de software	Atención de requerimientos de tecnología		2							4	
Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de facturación		2							4	
Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de ambientes				4				3		
Desarrollo, mantenimiento e implementación de software	Pruebas técnicas y de certificación				4			2			
Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a producción				4			2			
Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a pruebas		2					2			

PROCESO	FLUJOGRAMA	RESULTADO DE AUDITORIAS INDEPENDIENTES ANTERIORES					TIEMPO NO AUDITADO					30%	20%	18%	12%	15%	5%	PROMEDIO
		BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO							
		Informe limpio - Observaciones de Forma	Incumplimiento de Políticas y Procedimientos que afecten a la eficiencia y eficacia de los procesos/subprocesos. Proceso que no necesariamente debía ser evaluado en el ultimo año.	Incumplimiento regulatorio y de Política Interna	- Riesgo Reputacional - Existencia de un fraude. - Multas, sanciones que afecte a la calificación.	Observaciones determinadas afectan al negocio en marcha	Si el subproceso fue evaluado en el período de 0 a 6 meses	Si el subproceso fue evaluado en el período de 7 a 12 meses	Si el subproceso fue evaluado en el período de 13 a 19 meses	Si el subproceso fue evaluado en el período de 20 a 24 mes	Proceso no evaluado	FACTOR RO-1	FACTOR RO-2	FACTOR RO-3	FACTOR RO-4	FACTOR RO-5	FACTOR RO-6	
Desarrollo, mantenimiento e implementación de software	Atención de requerimientos de tecnología			3				2				3	4	2	4	3	2	3,09
Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de facturación			3							5	1	4	2	4	3	5	2,64
Desarrollo, mantenimiento e implementación de software	Determinación de inconsistencias de ambientes			3			1					1	4	4	3	3	1	2,68
Desarrollo, mantenimiento e implementación de software	Pruebas técnicas y de certificación		2					2				2	3	4	2	2	2	2,56
Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a producción		2				1					2	4	4	2	2	1	2,71
Desarrollo, mantenimiento e implementación de software	Traslado de desarrollo a pruebas		2				1					2	3	2	2	2	1	2,15

Elaborado por: Andrés Aguayo Yépez.

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	5
EXTREMO	1
CATASTRÓFICO	0
TOTAL	6

ANEXO No. 2 (c)

PROCESO	FLUJOGRAMA	CALIDAD DEL SISTEMA DE CONTROL INTERNO A TRAVES DE LA MATRIZ DE RIESGOS INSTITUCIONALES				
		BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
		Menores efectos que pueden ser facilmente remediados. Si el riesgo es bajo se administra con procedimientos rutinarios, si es insignificante no requiere ninguna acción.	Riesgo moderado y aceptable debe ser administrado con procedimientos normales de control.	Riesgo alto requiere de la atención de la alta Gerencia, planes de tratamiento requeridos, implementados y reportados a las líneas de supervisión.	Riesgo Extremo se requiere de acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.	Cuando se produce está en riesgo la continuidad del negocio.
Gestión de Seguridad de Información	Administración de Usuarios		2			
Gestión de Seguridad de Información	Administración y Autenticación de Backups Internos y externos		2			
Gestión de Seguridad de Información	Procedimiento de Control de Cambios	1				
Gestión de Seguridad de Información	Procedimiento para Reprocesos	1				

FLUJOGRAMA	COMPLEJIDAD DE LAS OPERACIONES E IMPACTO EN LOS PROCESOS CRITICOS DE LA ORGANIZACIÓN					NIVEL DE PRESION DE LA ADMINISTRACION PARA EL LOGRO DE OBJETIVOS ESTRATEGICOS				
	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	Riesgos que afectan superficialmente al proceso crítico y que pueden ser aceptados o facilmente superables en el tiempo.	Cuando el subproceso no consta en el detalle de "Procesos Críticos de la Organización"	Pérdida de eficiencia y calidad de ejecución en procesos críticos que generen riesgos por carga operativa adicional ocasionando: reprocesos y recuperación de datos por errores.	- Generen pérdida o fuga de información crítica, integridad y/o confiabilidad de información que es parte del core del negocio.	Cuando el subproceso consta en el detalle de "Procesos Críticos de la Organización"	Cuando el subproceso afecta de 0 a 2 objetivos estratégicos	Moderado 2 Cuando el subproceso afecta de 3 a 4 objetivos estratégicos	Cuando el subproceso afecta de 5 a 6 objetivos estratégicos	Cuando el subproceso afecta de 7 a 8 objetivos estratégicos	Cuando el subproceso afecta de 9 a más objetivos estratégicos
Administración de Usuarios				4					4	
Administración y Autenticación de Backups Internos y externos				4					4	
Procedimiento de Control de Cambios					5		2			
Procedimiento para Reprocesos				4			2			

FLUJOGRAMA	IMPACTO EN LAVADO DE ACTIVOS, EXPOSICION POLITICA Y PUBLICIDAD ADVERSA				
	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	No contar con un procedimiento formal para la difusión interna de documentación recibida de organismos de control (Nacionales e Internacionales).	Cuando el subproceso "NO" consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos"	- Desconocimiento de leyes y regulaciones. - No entrega de reportes requeridos por el organismo de control.	- Observaciones de los organismos de control que ocasionen el deterioro de la calificación de la entidad - Sanciones a accionistas o directores (destitución y multas).	Cuando el subproceso consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoría definido en el "Esquema Integral de Prevención y Control de Lavado de Activos" - Retiro de la franquicia.
Administración de Usuarios			3		
Administración y Autenticación de Backups Internos y externos				4	
Procedimiento de Control de Cambios		2			
Procedimiento para Reprocesos				4	

FLUJOGRAMA	RESULTADO DE AUDITORIAS INDEPENDIENTES ANTERIORES					TIEMPO NO AUDITADO				
	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO
	Informe limpio - Observaciones de Forma	Incumplimiento de Políticas y Procedimientos que afecten a la eficiencia y eficacia de los procesos/subprocesos. Proceso que no necesariamente debía ser evaluado en el ultimo año.	Incumplimiento regulatorio y de Política Interna	- Riesgo Reputacional - Existencia de un fraude. - Multas, sanciones que afecte a la calificación.	Observaciones determinadas afectan al negocio en marcha	Si el subproceso fue evaluado en el período de 0 a 6 meses	Si el subproceso fue evaluado en el período de 7 a 12 meses	Si el subproceso fue evaluado en el período de 13 a 19 meses	Si el subproceso fue evaluado en el período de 20 a 24 mes	Proceso no evaluado
Administración de Usuarios			3			1				
Administración y Autenticación de Backups Internos y externos			3			1				
Procedimiento de Control de Cambios			3							5
Procedimiento para Reprocesos			3							5

FLUJOGRAMA	30%	20%	18%	12%	15%	5%	PROMEDIO
	FACTOR RO-1	FACTOR RO-2	FACTOR RO-3	FACTOR RO-4	FACTOR RO-5	FACTOR RO-6	
Administración de Usuarios	2	4	4	3	3	1	2,98
Administración y Autenticación de Backups Internos y externos	2	4	4	4	3	1	3,10
Procedimiento de Control de Cambios	1	5	2	2	3	5	2,60
Procedimiento para Reprocesos	1	4	2	4	3	5	2,64

Elaborado por: Andrés Aguayo Yépez.

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	3
EXTREMO	1
CATASTRÓFICO	0
TOTAL	**4**

ANEXO No. 2 (d)

		CALIDAD DEL SISTEMA DE CONTROL INTERNO A TRAVES DE LA MATRIZ DE RIESGOS INSTITUCIONALES					COMPLEJIDAD DE LAS OPERACIONES E IMPACTO EN LOS PROCESOS CRITICOS DE LA ORGANIZACION					NIVEL DE PRESION DE LA ADMINISTRACION PARA EL LOGRO DE OBJETIVOS ESTRATEGICOS					IMPACTO EN LAVADO DE ACTIVOS, EXPOSICION POLITICA Y PUBLICIDAD ADVERSA					RESULTADO DE AUDITORIAS INDEPENDIENTES ANTERIORES					TIEMPO NO AUDITADO											
		BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTRÓFICO	30%	20%	18%	12%	15%	5%	
PROCESO	FLUJOGRAMA	Menores efectos que pueden ser fácilmente remediados. Si el riesgo es identificado puede ocasionar reprocesos, tolerancia, si es insignificante no requiere ninguna acción.	Riesgo moderado y manejable, debe ser administrado con procedimientos normales de control.	Riesgo alto requiere de la atención de la alta Gerencia, planes de tratamiento requeridos, implementados y reportados a las líneas de supervisión.	Riesgo Extremo se requiere de acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.	Cuando se produce esta en riesgo la continuidad del negocio.	Riesgo que afecten significativamente el proceso crítico y que pueden ser aceptados o facilmente superables en el tiempo.	Cuando el subproceso no consta en el Organigrama de Procesos Críticos de la Organización.	Pérdida de eficiencia y calidad de procesos críticos de la organización que generen reprocesos por carga operativa adicional ocasionando reprocesos y desatención de clientes prioritarios.	Generen pérdida o fuga de información crítica para la entidad y/o, contabilidad de información que es parte del core del negocio.	Cuando el subproceso consta en el detalle de "Procesos Críticos de la Organización"	Cuando el subproceso afecta de 0 a 2 objetivos estratégicos	Moderado 2 Cuando el subproceso afecta de 3 a 4 objetivos estratégicos	Cuando el subproceso afecta de 5 a 6 objetivos estratégicos	Cuando el subproceso afecta de 7 a 8 objetivos estratégicos	Cuando el subproceso afecta de 9 a mas objetivos estratégicos	No contar con un procedimiento formal para la difusión interna de documentos (normas internacionales).	Cuando el subproceso "NO" consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoria definido en el Sistema Integrado de Prevención y Control de Lavado de Activos" - Desconocimiento de leyes y regulaciones - No envíos de reportes requeridos por el organismo de control.	Observaciones de los organismos de control que ocasionen el deterioro de la calificación de la entidad (suspensión y multas).	Cuando el subproceso consta en el detalle de procesos y subprocesos establecidos para monitoreo por parte del área de Auditoria definido en el Sistema Integrado de Prevención y Control de Lavado de Activos" - Retiro de la franquicia.	Observaciones determinadas afectan el negocio en materia	Informe limpio - Observaciones de Forma	Incumplimiento de Políticas y Procedimientos que afecten a la eficiencia y eficacia de los procesos críticos. Proceso que no necesariamente debió ser evaluado en el último año.	Incumplimiento regulatorio y de Política Interna	Riesgo Reputacional - Existencia de un Fraude. - Multas, sanciones que afecte a la utilidad.	Observaciones determinadas afectan el negocio en materia	Si el subproceso fue evaluado en el período de 4 a 6 meses	Si el subproceso fue evaluado en el período de 7 a 12 meses	Si el subproceso fue evaluado en el período de 13 a 19 meses	Si el subproceso fue evaluado en el período de 20 a 24 mes	Proceso no evaluado	FACTOR RO-1	FACTOR RO-2	FACTOR RO-3	FACTOR RO-4	FACTOR RO-5	FACTOR RO-6	PROMEDIO
Gestión Soporte a Usuarios	Atención de requerimientos			3					3						4					4			2				2				3	3	4	4	2	2	3,10
Gestión Soporte a Usuarios	Atención helpdesk			3					3						4					4			2				2				3	3	4	4	2	2	3,10
Gestión Soporte a Usuarios	Atención requerimientos WEB	1							3						4					4			2							5	1	3	4	4	2	5	2,65
Gestión Soporte a Usuarios	Creación de usuarios de correo electrónico	1								4			2							4				3			2				1	4	2	4	3	2	2,49
Gestión Soporte a Usuarios	Eliminación de usuarios de correo electrónico	1								4			2							4				3			2				1	4	2	4	3	2	2,49
Gestión Soporte a Usuarios	Entrega de reportes por requerimiento de usuario			3						4					4					4			2							5	3	4	4	4	2	5	3,45
Gestión Soporte a Usuarios	Generación de informes			3					3						4					4			2							5	3	3	4	4	2	5	3,25
Gestión Soporte a Usuarios	Preparación de equipos	1							3				2				1						2				2				1	3	2	1	2	2	1,78
Gestión Soporte a Usuarios	Revisión de actualización del sistema operativo		2							4			2					2					2				2				2	4	2	2	2	2	2,40
Gestión Soporte a Usuarios	Revisión de definiciones antivirus	1									5		2						3					3			2				1	5	2	3	3	2	2,57

Elaborado por: Andrés Aguayo Yépez.

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	1
ALTO	5
EXTREMO	4
CATASTRÓFICO	0
TOTAL	10

ANEXO No. 2 (e)

		CALIDAD DEL SISTEMA DE CONTROL INTERNO A TRAVES DE LA MATRIZ DE RIESGOS INSTITUCIONALES					COMPLEJIDAD DE LAS OPERACIONES E IMPACTO EN LOS PROCESOS CRITICOS DE LA ORGANIZACIÓN					NIVEL DE PRESION DE LA ADMINISTRACION PARA EL LOGRO DE OBJETIVOS ESTRATEGICOS					IMPACTO EN LAVADO DE ACTIVOS, EXPOSICION POLITICA Y PUBLICIDAD ADVERSA					RESULTADO DE AUDITORIAS INDEPENDIENTES ANTERIORES					TIEMPO NO AUDITADO											
		BAJO	MODERADO	ALTO	EXTREMO	CATASTROFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTROFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTROFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTROFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTROFICO	BAJO	MODERADO	ALTO	EXTREMO	CATASTROFICO	30%	20%	18%	12%	15%	5%	
PROCESO	FLUJOGRAMA	Hallazgos efectos que pueden ser subsanados o remediados. Si el riesgo es por incumplimiento con procedimientos rutinarios, o es insignificante no requiere ninguna acción.	Riesgo moderado y / aceptable debe ser administrado con procedimientos normales de control.	Riesgo alto requiere de la atención de la alta Gerencia, planes de tratamiento requeridos, implementados y reportados a las líneas de supervisión.	Riesgo Extremo se requiere de acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.	Cuando se produce esta en riesgo la continuidad del negocio	Riesgos que afectan superficialmente al proceso crítico y/que pueden ser asumidos o fácilmente superables sin cambios	Cuando el subproceso no consta en el mapa de Proceso Crítico de la Organización"	Pérdida de eficiencia y calidad de ejecución en procesos críticos que generen riesgos por carga operativa, demoras en los procesos, reprocesos y recuperación de dato por errores.	Generen pérdida o fuga de información crítica, integridad y/o confidencialidad de información que es parte esencial del negocio	Cuando el subproceso consta en el mapa de Proceso Crítico de la Organización"	Cuando el subproceso afecta de 0 a 2 objetivos estratégicos	Moderado 2 Cuando el subproceso afecta de 3 a 4 objetivos estratégicos	Cuando el subproceso afecta de 5 a 6 objetivos estratégicos	Cuando el subproceso afecta de 7 a 8 objetivos estratégicos	Cuando el subproceso afecta de 9 a mas objetivos estratégicos	No contar con un procedimiento formal de archivo y manejo de documentación recibida de organismos de control (Nacionales e internacionales)	Cuando el subproceso "NO" contiene en el diseño de procesos y subprocesos establecidos para prevenir y detectar actividades de Auditoria definido en el "Esquema Integral de Prevención y Control de Lavado de Activos"	No cumplimiento de leyes y regulaciones. - No entrega de reportes requeridos por el organismo de control.	Observaciones de los organismos de control que ocasionen el deterioro de la calidad y la imagen de la entidad. - Sanciones a accionistas o directores (destitución y multas).	Cuando el subproceso consta en el detalle de procesos y subprocesos del mapa de procesos de la entidad del área de Auditoria definido en el "Esquema Integral de Prevención y Control de Lavado de Activos" - Retiro de la franquicia.	Informe limpio - Observaciones de forma	Incumplimiento de Políticas y procedimientos que afecten a la ejecución normal de los procesos/subprocesos Proceso que no necesariamente afecta la misión del negocio	Incumplimiento regulatorio y de Política interna	Riesgo Reputacional - Existencia de un fraude. - Multa o sanción que afecte a la calificación.	Observaciones determinantes afectan el negocio en marcha	Si el subproceso fue evaluado en el periodo de 0 a 6 meses	Si el subproceso fue evaluado en el periodo de 7 a 12 meses	Si el subproceso fue evaluado en el periodo de 13 a 18 meses	Si el subproceso fue evaluado en el periodo de 19 a 24 meses	Proceso no evaluado	FACTOR RO-1	FACTOR RO-2	FACTOR RO-3	FACTOR RO-4	FACTOR RO-5	FACTOR RO-6	PROMEDIO
Monitoreo de Sistemas y Aplicaciones	Monitoreo de servicios, sistemas y aplicaciones			3							5			2							4						3					3	5	2	4	3	1	3,24
Procesamiento Tecnológico	Parametrizaciones		2							4					4						4					1					2	4	4	4	4	1	3,25
Procesamiento Tecnológico	Procesamiento de transacciones y disponibilidad de información			3							5				4					5							2				3	5	4	5	4	2	3,92
Procesamiento Tecnológico	Seguimiento y paso a producción		2						3						4							2				1				2	3	4	4	2	1	2,75

Elaborado por: Andrés Aguayo Yépez.

CALIFICACION	NUMERO DE PROCESOS
BAJO	0
MODERADO	0
ALTO	1
EXTREMO	3
CATASTRÓFICO	0
TOTAL	4