UNIVERSIDAD IBEROAMERICANA

Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial
Del 3 de abril de 1981

“EL MERCADO DE VALORES EN EL ECUADOR Y SU ADMINISTRACIÓN INTEGRAL DE LOS RIESGOS DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN”.

TESIS

Que para obtener el grado de

MAESTRA EN ADMINISTRACIÓN DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN

Presenta

MARÍA DEL CARMEN FREIRE MERCHÁN

Director: Mtro. Jorge Garibay

Lectores: Dr. Héctor Fragoso

Dr. Alfonso Miguel

México, D.F. 2012

ÍNDICE

Índice de contenidos

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

AGRADECIMIENTOS

Este trabajo se realizó en la Universidad Iberoamericana de Ciudad de México, Departamento de Sistemas, Programa de Maestría en Administración de Servicios de Tecnologías de Información entidad a la cual le estoy muy agradecida por haberme hecho parte de tan prestigiosa institución y conté con el apoyo financiero de la Secretaría Nacional de Ciencia y Tecnología de Ecuador, desde aquí agradezco al gobierno ecuatoriano por este fundamental apoyo, por permitirme ser parte de una generación de triunfadores y gente productiva para el país.

Quiero agradecer ante todo a Jehová Dios, el Todopoderoso, porque gracias a él tuve la oportunidad de realizar tan prestigioso honor como es la Maestría en Administración de Tecnología de Información, a él le debo mi vida, profesión, familia y amigos. Por haberme dado salud, sabiduría para lograr mis objetivos, además de su infinita misericordia, gracia, bondad y lo principal amor.

A mi Coordinador del programa de Maestría, Dr. Pedro Solares Soto, por el apoyo y su ayuda en numerosas ocasiones, su disponibilidad y amabilidad que siempre demostró para mi persona considerando mi situación académica y mi calidad de extranjera.

A mi director de tesis, Mtro. Jorge Garibay, por compartir conmigo su interés y sus valiosos conocimientos, por la formación que me proporcionó, por su orientación siempre impecable y precisa, por su dedicación, apoyo técnico y académico en todo momento y especialmente por su calidad humana y pedagógica, gracias por la riqueza de sus enseñanzas.

Al llegar a la Universidad Iberoamericana no puedo dejar de recordar el apoyo del profesorado del Programa de Maestría en Administración de TI y en particular de aquellos que me proporcionaron su contingente humano y académico como fueron: Dr. Héctor Fragoso, Ing. Fernando Mar, Dr. Ramón Marín y Dr. Alejandro Canales. Gracias por su ayuda y comprensión.

Al Mtro. Carlos Zamora por su gran apoyo en haberme brindado la oportunidad de realizar prácticas profesionales en su honorable y prestigiosa empresa Conseti S.A. , por medio de la cual obtuve experiencia laboral en el área de consultoría y auditoría de TI.

A mis compañeros de Maestría que mutuamente nos apoyamos en nuestra formación profesional me ayudaron y acompañaron en este largo camino y lo hicieron mucho más fácil y agradable.

A mi familia, sobre todo a mis hijos por quienes he dado todo mi esfuerzo y dedicación, le agradezco su cariño, amor y comprensión que cada día me ofrecen. Por los millones de sacrificios que han hecho para que pueda alcanzar aquello que desde el principio fue un milagro y bendición de Dios. Porque entiendo y siento lo que significa para ellos que yo esté aquí, en esta etapa ahora. Por todo ello, Paula, Isaac e Isaías, este paso es de y para ustedes, se los dedico a ustedes la bendición más grande y completa que me ha dado el Señor.

A mi tía Vilma Merchán y amiga María Elena Cisneros quienes me apoyaron incondicionalmente y me brindaron su garantía confiando 100% en mi persona, quienes no escatimaron ni sus bienes materiales para poder servirme, gracias desde el fondo de mi corazón.

Por último a ti, Salvador, por animarme cada día en estos últimos dos años, con tus oraciones, con tu cariño, comprensión, amor. Porque sobre ti recayeron mis peores momentos, por aguantarme cuando ya ni yo lo podía hacer, por los sacrificios que pasaste por mí. Por tu ayuda incondicional y tu fortaleza en todas y cada una de las etapas de la maestría. Porque eres muy importante para mí y espero poder retribuirte a lo largo de nuestra vida todo lo que me diste, todo lo que me das.

RESUMEN

El tema de la presente tesis se eligió debido a que es un asunto en el cual no se han desarrollado investigaciones en mi país, Ecuador, y el cual está sobresaliendo en estas épocas. A lo largo del desarrollo de esta tesis se habla de que el mercado de valores constituye el mayor porcentaje de la economía en Ecuador, como claramente las publicaciones de diarios y revistas de primera circulación indican. Resaltando entre ellos:

"De acuerdo al estudio del comportamiento de las empresas privadas con relación al mercado de valores en el Ecuador, el Banco Central del Ecuador, la revista el financiero entre otras revistas financieras, indican que el mercado de valores ha ido creciendo tanto en número de emisiones, como en montos negociados. En los cuatro primeros meses del año se negociaron 1780 mil 309 millones de dólares.[1]

"Las empresas privadas ven a la Bolsa de Valores como su nueva fuente de financiamiento. La emisión de obligaciones, la titularización y la negociación de papeles comerciales son los mecanismos con los cuales se obtienen recursos para financiar planes de expansión o capital de trabajo".

También se ha vuelto más fácil encontrar clientes o inversionistas, sobre todo del sector público. "Hay un plan agresivo de entidades públicas con exceso de liquidez que son los compradores. Los inversionistas privados y administradores de fondo también han participado activamente. Hace cuatro o seis años atrás se tomaba un poco más tiempo conseguir a los clientes que compren. Ahora no toma más de dos meses. Hay casos en que se hace en una semana o 15 días, y al final se colocan el 100 por ciento".[2]

Considerando esta particularidad, he analizado la importancia y necesidad de darle relevancia a una efectiva administración de riesgos asociados a la tecnología de información (en adelante T.I). También se hace referencia a las tendencias de la tecnología y como se emplean en el mercado de valores ecuatoriano, que en la mayoría de los casos no aprovechan eficientemente los recursos de T.I. que tienen a su alcance y no se dan cuenta de las ventajas y/o beneficios que pueden obtener al implementar controles o mejorar los que ya tienen implementados para el manejo de sus recursos tecnológicos.

Para llevar a cabo este trabajo de investigación se abordan temas desde conceptos generales: Mercado de Valores en el Ecuador comparado con la institución Indeval en México, análisis y entorno global, panorama general de los riesgos asociados a las T.I. Gestión de riesgos de T.I., metodología y modelo de aplicación de los riesgos de T.I., en un proceso de negocio dentro del mercado de valores. También se procederá al análisis de la problemática de la auditoría de riesgos de T.I., la legislación a nivel nacional e internacional que regula esta función así mismo la forma de adaptarlas a los marcos de referencia de mejores prácticas y la tecnología adecuada.

[1] (Gestiopolis, julio 2009)
[2] (Diario de negocios Hoy, Quito, Ecuador, 25 Sept.2009)

El objetivo de esta investigación es determinar cuál es la importancia de la función de la Administración de riesgos asociados a las tecnologías de información dentro del mercado de valores y proponer un modelo que sirva de guía para la definición, implementación y control de dicha función, llevando a cabo el caso práctico aplicando todos los conocimientos adquiridos a lo largo del desarrollo de la Maestría en Administración de Servicio de la Tecnología de Información, si se logró el objetivo que en este caso en particular es satisfactorio y obteniendo la experiencia y práctica.

De igual manera se tratan temas de cómo debe estar conformada una oficina de administración de riesgos de T.I. conforme a las necesidades del mercado de valores en el Ecuador, se indicará su definición, conformación, estructura organizacional, las funciones que desempeñará esta área, las metodologías, herramientas y marcos de referencia que soportan este análisis y para finalizar se menciona el perfil del líder de esta área.

Profundizando el tema de metodología y herramientas se menciona que el proceso empieza con la descripción de las actividades relacionadas con la gestión de riesgos asociados a las T.I. , iniciando desde la revisión preliminar, evaluación, objetivos y alcance con apego a los estándares internacionales como son: ISO-27005, Risk IT, Cobit , entre otros , análisis de las políticas de seguridad, identificación de vulnerabilidades, amenazas, riesgos y sus correspondientes impactos relacionados con las T.I., pruebas del cumplimiento de esta propuesta de implementación, evaluación y control de la administración de riesgos de T.I. en el mercado de valores ecuatoriano.

Para comprobar la consecución de los objetivos planteados anteriormente, se realiza un caso práctico en el cual se aplica el modelo propuesto de la presente tesis, en este caso se demuestran los resultados obtenidos de la aplicación del modelo dejando establecido cuál es la importancia de la función de la administración de riesgos de T.I. Definiendo e implementando esta función, llegando a demostrar si el resultado es satisfactorio o si no lo es consiguiendo una conclusión del tema.

Para finalizar el tema se concluye que se logró el objetivo propuesto, en el cual el caso práctico demuestra la importancia de la Administración de riesgos de T.I. en el mercado de valores, con ello se identifican los principales riesgos del negocio y de igual forma se sugiere la estructuración del área de gestión de riesgos en T.I., continuando con auditorías constantes para llegar a implementar el área de forma definitiva.

INTRODUCCIÓN

En la actualidad las estadísticas del Banco Central del Ecuador y la Superintendencia de Bancos, órganos reguladores del mercado de valores en el Ecuador, concluyen que es un motor económico muy importante en el país, está conformada en su mayoría de bolsas y casas de valores, por lo que surge la necesidad de invertir en sistemas de tecnología de información actualizados y con la respectiva seguridad de los riegos de esta tecnología, sin embargo la mayoría de estas instituciones carecen de controles eficientes o de una adecuada gestión de riesgos en T.I., aunado a esto los marcos reguladores eficientes y que se basan en las mejores prácticas en el manejo de los riesgos de T.I., por lo que el hecho de promover esta investigación es realizar un proceso eficiente metodológico y sistematizado en administración de riesgos respaldado en dichos marcos, aunque resulta una inversión no sustentable de capital para el mercado de valores ecuatoriano.

Así mismo, en la actualidad, se está aprobando en el Congreso Nacional del Ecuador, la Ley de Mercado de Valores, enmarcada a los estándares internacionales y con la incorporación de una entidad denominada Central de Contraparte, cuya función primordial será la Custodia centralizada de los títulos y valores tanto de la empresa pública y privada del país, entre otras funciones.

Con esta resolución se establece claramente la importancia que para el gobierno ecuatoriano tiene que el sistema donde se desarrollan las actividades del mercado de valores sea segura, robusta y eficiente, pero pese a existir el apoyo gubernamental, se ha dejado de lado o se le ha restado importancia que la función de Administración de riesgos en T.I., cumple un rol muy decisivo en el mercado de valores. Por otra parte la inexistente legislación ecuatoriana que contemple y que obligue la existencia de la administración de riesgos en T.I. como un órgano de control interno ha dado lugar a que los participantes del mercado de valores omitan esta función, delegando la responsabilidad a otras áreas.

Es por ello que el objetivo de esta investigación es determinar y establecer cuál es la importancia de una adecuada administración de riesgos asociados a las tecnología de información y promoverla basándose en los marcos de referencia con lo cual se logrará tener una visión objetiva y más amplia que les permitirá a este mercado tener un punto de referencia para la implementación de controles o mejorar los que ya se han implementado para lograr un mejor aprovechamiento de la Administración de las tecnologías de información.

Para objeto de esta investigación se desarrollarán 6 capítulos , los cuales incluye el marco metodológico, conceptos de riesgos operativos ya que dentro de este tipo de riesgos se desprenden los riesgos de las tecnologías de información, características e importancia, la problemática de la administración de riesgos dentro del mercado de valores en el Ecuador, además de los temas relacionados a la legislación, mejores prácticas y tecnología, para poder así desarrollar la presente tesis de la importancia y propuesta de creación y desarrollo de un modelo eficiente y acorde al mercado de administración de riesgos de T.I., así como el relato de un caso práctico donde se aplican los temas ya previamente mencionados.

El trabajo se divide en dos partes: La primera comprende 3 capítulos y aborda cuestiones generales sobre el funcionamiento de los mercados de valores Ecuador y México con su respectiva administración de riesgos.

En el capítulo I , Marco metodológico se encuentra la descripción del marco metodológico, además se pretende explicar la problemática que existe en el sector del mercado de valores a nivel organizacional , así como los objetivos que se quieren lograr con la propuesta de esta tesis y la justificación del porque se escogió este tema, utilizando diferentes herramientas para su comprobación.

El capítulo II tiene como objetivo caracterizar de manera general la evolución y los principales conceptos que involucran el funcionamiento del mercado de valor ecuatoriano y su comparación con el modelo mexicano de la Central de Contraparte de Valores (en adelante CCV).

El tercer capítulo realiza una descripción detallada del riesgo y sus respectivos enfoques. Entre sus propósitos está ofrecer una composición de lugar que ubique los riesgos de tecnología de información en un marco general aplicable a cada proceso de negocio del mercado de valores en el Ecuador. Aporta un marco teórico conceptual de la administración de riesgos. Estudia la problemática de los riesgos de T.I. y su relevancia dentro del mercado de valores.

La segunda parte se compone de tres capítulos y se dedica a la gestión y aplicabilidad del modelo esquemático de una administración integral de riesgos de tecnología de información dentro de un proceso en específico.

El capítulo IV, metodología de administración de riesgos de T.I. basados en marcos de referencia y a la utilización de estándares como ((ISO 31000, Risk IT, COBIT, ISO 27005, entre otros) que contemplan la función de gestión de riesgos en T.I., así como los procesos desde la planeación estratégica, esto significa la metodología más acorde para el mercado objeto de estudio. Importancia y propuesta de la creación de una oficina de administración de riesgos asociados a las tecnologías de información.

En el capítulo V, estudio y análisis del modelo de Deming, sus componentes y aplicación dentro del modelo de gestión de riesgos de T.I. Se desarrollará el impacto que tiene principalmente en la misión y en los resultados de la compañía, los mismos que deben de ser alineados, medibles y comunicables por medio de indicadores de tiempo, recursos y alcance. La importancia como marco de mejora continua radica en que los directivos pueden diagnosticar, decidir, planear y controlar el rumbo para alcanzar los objetivos.

El capítulo VI, tiene como objeto exponer los resultados obtenidos de la implementación del modelo de administración de riesgos de T.I. propuesto y aplicado a un proceso dentro del modelo de negocios del mercado, demostrando la importancia de la función, así como los beneficios que esto genera y ayuda en la toma de decisiones con respecto a las tecnologías de información que los altos directivos de las empresas que conforman el mercado de valores deben de realizar.

Se concluye la tesis con el propósito de concientizar a los participantes en el mercado de valores ecuatoriano con respecto a la determinación e importancia de una eficiente administración de riesgos asociados a las T.I. y beneficios que aporta la inversión en estos controles de forma continua, reconociendo que es una oportunidad de crecimiento y competitividad para las empresas que lo apliquen, evidenciando estos beneficios mediante los resultados que arrojen la implementación del modelo propuesto.

De forma general, la tesis propone un análisis que integra los aspectos teóricos y técnicos con su utilidad y aplicación en la práctica, a partir de un enfoque crítico que persigue determinar la conveniencia y eventuales formas de aplicación de estos instrumentos. Contribuye también desde el punto de vista metodológico, integralidad y sistematicidad del proceso.

Por lo general, reducir los riesgos es una necesidad para todos los agentes que intervienen en estas operaciones. Cuando en ellas va involucrado el futuro de una empresa, institución y país, más que una necesidad, minimizar los riesgos se convierte en una obligación.

PRIMERA PARTE: EL MERCADO DE VALORES EN EL ECUADOR Y SUS RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

CAPÍTULO I.- MARCO METODOLÓGICO

Dentro de este capítulo, se encuentra la descripción del marco metodológico, además se pretende explicar la implementación, evaluación y control del área de administración de riesgos relacionados a la T.I. aplicable a los procesos de negocios que realizan los participantes del mercado de valores dentro de cada empresa, la problemática que existe al no tenerla y sus implicaciones, desde el punto de vista organizacional, así como los objetivos que se quieren lograr en la propuesta de esta tesis y por último la justificación del porque se escogió este tema. Se utilizan eficientes herramientas para su comprobación. Se sustenta tal problemática por medio de cuadro metodológico integral del desarrollo del proyecto de tesis.

A continuación se lista el contenido temático de este capítulo:

1.1.- PLANTEAMIENTO DEL PROBLEMA

El mercado de valores en el Ecuador está regido por 2 grandes grupos, ubicados en las ciudades de Quito y Guayaquil, el primer grupo corresponde a las Bolsas de Valores en las que se puede distinguir claramente la organización y la estructura misma, las cuales se desarrollan dentro del mercado bursátil y a la vez económico y por otro lado aquellas instituciones como son las: Casas de Valores, Depósitos Centralizado de Valores (DECEVALE), administradoras de fondos y bancos, es predominante este grupo y se caracteriza por la gestión enfocada a la colocación de títulos sin realizar un eficiente control de riesgos financieros, operativos y dentro de éste último los avances en las tecnologías de información , lo que será materia del estudio en este trabajo, se ha identificado e investigado que las instituciones indicadas no prestan demasiada atención al costo de oportunidad de capital o a la inversión que le permitirá esta implementación de gestión de riesgos en el crecimiento del mercado de valores en general.

Para estos dos grupos la información y las tecnologías que la soportan representan recursos de gran valor para las mismas llegando a convertirse en indispensable. Por eso la seguridad de este elemento deberá ser notable y eficiente.

Actualmente, la seguridad que involucra las tecnologías de información, no se le ha dado la importancia necesaria en el Ecuador, dado a que existe una falta de conciencia en esta materia.

Por lo tanto éste trabajo de tesis, se realizó con la finalidad de proponer una metodología dirigida para las empresas del sector de mercado de valores que quieren mejorar o evitar una situación de riesgo a todo nivel, por tener un escaso conocimiento en la materia de seguridad de la información en esta área.

Su propósito es que mediante el establecimiento de objetivos y actividades que permitan alcanzarlos, se debe de crear un ambiente de seguridad en la información contenida en las tecnologías de información.

Durante el desarrollo de este proyecto de tesis se detallan cada uno de los pasos que establece la metodología propuesta y se explican las actividades que se desarrollan y al final de este trabajo escrito se presenta un ejemplo de su aplicación.

Por lo tanto se muestra un mercado sistémico y metodológico en el que se descubre una serie de funciones a emplear sus correspondientes técnicas, herramientas y productos a obtener para realizar el desarrollo del proyecto de tesis.

ILUSTRACIÓN 1. MARCO METODOLÓGICO INTEGRAL PARA EL DESARROLLO DE PROYECTO DE TESIS

ACTIVIDADES ¿Qué hacer?	TÉCNICAS ¿Cómo hacerlo?	HERRAMIENTAS ¿Con qué hacerlo?	METAS ¿Qué obtener?
1.- Definir el tema	Observación/investigación	Método científico	Especificar la oportunidad ó problemática a considerar en esta investigación
2.- Recopilar información	Investigar/Recopilar Información	Libros, estándares internacionales, marcos de referencia, revistas, internet	Identificar y aislar la problemática y oportunidad para obtener una visión sistémica del tema de estudio
3.- Desarrollar el marco metodológico	Definición del marco metodológico, mediante una tabla	Procesador de palabras	Definir las actividades que se tienen que hacer para realizar el proyecto de tesis
4.- Definir el marco conceptual	Observación/Investigación, Recopilación Bibliográfica, Definición del marco conceptual	Libros, estándares internacionales, marcos de referencia, Enciclopedias, diccionarios, Pirámide conceptual, internet , entrevistas a funcionarios de la Bolsa Mexicana de Valores(B.M.V)	Delimitar los conceptos y describir los términos generales empleados en el proyecto de tesis
5.- Identificar y analizar la situación actual **5.1. Definir la justificación** **5.2. Definir objetivos: general y específicos**	Definir una visión global del tema en cuestión a tratar. Conocer conceptos básicos para la definición de objetivos	Libros, estándares internacionales, Internet, Procesador de palabras	Obtener un análisis de las ventajas y desventajas de la metodología propuesta y modelos de buenas prácticas existentes en el mercado. A partir del análisis, realizar una justificación lógica que defienda el estudio del proyecto en cuestión. Definir los alcances o resultados a obtener.
6.- Desarrollar la metodología	Investigación/ Analizar, identificar y definir la metodología de desarrollo	Libros, marcos de referencia, estándares internacionales, internet, entrevistas	Obtener el conjunto de actividades que conforman la metodología a desarrollar
7.- Construcción de un modelo	Definir las partes que conforman el modelo a seguir	Procesador de palabras	Concebir un modelo a seguir con el conjunto de actividades definidas anteriormente
8.- Redactar el documento de tesis	Conocer la metodología para el desarrollo y redacción de un proyecto de tesis de maestría	Procesador de textos, editor de imágenes, hoja de cálculo, entre otros	Obtener un documento escrito del proyecto de tesis
9.- Presentar el examen de grado	Investigar los lineamientos institucionales de la Univ. Iberoamericana para presentar el examen de grado	Internet Entrevista	Conseguir el grado de Maestra en Administración de Servicios de Tecnología de Información.

Las empresas que conforman el mercado secundario, siendo éstas: Casas de Valores, Administradoras de Fondos, Bancos y demás instituciones financieras, representan un aporte muy importante al desarrollo financiero y económico del Ecuador, por lo que se debe prestar un notable interés en el desarrollo y competitividad de las mismas.

Debido al mercado que es cada vez más abierto y global este tipo de empresas, han tenido que buscar maneras de mantenerse a flote. Una de estas, es mediante el uso de las T.I., pero debido a que no existe un marco de referencia como tal adecuado a sus necesidades y debido también a factores primordiales como la falta de información, desconfianza, inercia o carencia de recursos los cuales impiden a las mismas a dar el paso para adquirir tecnología e inclusive no contar con las herramientas necesarias para obtener un mejor provecho de las mismas como parte del servicio que ofrece el negocio.

Actualmente las condiciones del mercado permiten a las empresas en referencia ver la inversión en tecnología como una oportunidad de crecimiento y competitividad, no obstante el factor de cómo medir, evaluar y controlar los riesgos de la tecnología de información con las que se cuenta actualmente y con las que se pretende adquirir, por este motivo en particular se realiza esta investigación cuyo objetivo es determinar la función de la Administración de Riesgos asociados a la tecnología de información y promover un modelo de control de gestión de riesgos orientados a las T.I. y la correspondiente estructuración de la oficina de administración de riesgos con su líder de seguridad informática, llamado CISO[3].

La función de la Administración de riesgos asociados a las T.I. implica la verificación de lo "que es" contra lo que "debe de ser", desde un enfoque fiscalizador. Aunque actualmente se carece de un marco jurídico que satisfaga el respaldo de observaciones o inconsistencias que pueden afectar a la continuidad en la función de las tecnologías de información y en el peor de los casos, la evidencia documental que se llega a recopilar, en muchos de los casos es descalificada como "suficiente y competente" por las autoridades en procesos de posibles faltas a la ley.

Si bien es cierto que la función de la Administración de riesgos, cualquiera que sea el campo de acción (operativo, financiero, mercado, legal, para citar los principales) debe tener como propósito principal ser una función principalmente "de detección" no tanto "correctiva", en caso de detectarse por ejemplo mal uso o abusos de equipos de cómputo, esquemas de seguridad de las T.I., fraudes, espionaje, robo, pérdida o daño de la información de la institución, etc.

1.2.- OBJETIVOS

Los objetivos son una parte crucial para determinar la importancia de la tesis, es decir, comprobar la razón de ser del proyecto, los cuales a partir del objetivo principal se desglosan los demás objetivos específicos. Los objetivos de la investigación presente, se exponen de manera clara y precisa, para dar a entender el logro que se desea obtener con la realización de esta tesis.

[3] CISO(Chief Information Security Officer)

1.2.1.-OBJETIVO GENERAL

Determinar la importancia de la función de la Administración de Riesgos asociados a la T.I. dentro de las empresas participantes en el mercado de valores y proponer un modelo que sirva de guía para la definición e implementación de dicha función, compuesto de un conjunto de buenas prácticas, controles y checklists basado en los marcos y los estándares de metodologías de gestión de riesgos en tecnología de información ya existentes.

Proponer una metodología para obtener un sistema ó medio ambiente basado en objetivos de control y sus actividades correspondientes para crear un medio de seguridad de información operada por las Tecnologías de Información para aquellas empresas que cuenten con una estructura y organización formal.

1.2.2.- OBJETIVOS ESPECÍFICOS

- Identificar y conocer el medio ambiente general del mercado de valores para determinar el marco contextual y conceptual de la situación en estudio.
- Determinar la importancia de la función de la Administración de riesgos asociados a las T.I. y los beneficios de dicha área dentro de la empresa.
- Analizar, evaluar y diagnosticar la situación actual con respecto a los marcos de referencia y control interno para obtener un sistema que cree un medio ambiente de seguridad de la información que es operada por las Tecnologías de Información.
- Proponer la metodología para el uso de objetivos de control y sus actividades como medio de seguridad de la información albergada en las tecnologías de información con la finalidad de reducir el escaso conocimiento en esta materia.
- Implementar la metodología en un proceso de “La empresa” y evaluar el desempeño de las actividades de control y sus objetivos ya aplicados.

1.3.- TÉCNICAS E INSTRUMENTACIÓN DE MEDICIÓN

Para sustentar el desarrollo de esta tesis se recurrió a las técnicas e instrumentación que a continuación se listan:

1.3.1.- EXPLORATORIA

La investigación exploratoria se define como la recolección de información mediante mecanismos informales y no estructurados. Se propone obtener datos y hacer observaciones básicas que permitan delimitar un problema. Esta investigación está diseñada para obtener un análisis preliminar de la situación con un mínimo costo y tiempo.

Esta investigación tiene por objeto que el investigador se familiarice con la situación del problema, identifique las variables más importantes, reconozca otros cursos de acción proponga pistas idóneas para trabajos posteriores y puntualice cuál de estas posibilidades tiene la máxima prioridad en la asignación de los escasos recursos presupuestarios de la empresa. La finalidad de los estudios exploratorios es ayudar a obtener, con relativa rapidez, ideas y conocimientos en una situación.

La investigación exploratoria es adecuada en situaciones de reconocimiento y definición del problema. Una vez que el problema se ha definido claramente la investigación exploratoria puede ser útil para la identificación de cursos alternativos de acción.

- Recolectar la información necesaria de fuentes de información
- Analizar y clasificar la información obtenida
- Filtrar y estructurar dicha información
- Adecuar la información para el desarrollo de la investigación
- Determinar la importancia de la función de la Administración de riesgos asociados en las T.I.
- Desarrollar un modelo de función de gestión de riesgos en T.I. en base a la información recabada**.**

1.3.2.- DOCUMENTALES

La técnica documental permite la recopilación de información para enunciar las teorías que sustentan el estudio de los fenómenos y procesos, incluye el uso de instrumentos definidos según la fuente documental a que hacen referencia. Consiste primordialmente en la presentación selectiva de lo que expertos ya han dicho o escrito sobre un tema determinado. Además puede presentar la posible conexión de ideas entre varios autores y las ideas del investigador.

1.4.- ALCANCE

El alcance de la investigación establecerá el estado de la situación actual de la administración de riesgos de TI en el Ecuador vs México en el mercado de valores, adaptando un modelo que permita al sector de referencia en el Ecuador ser más confiable y eficaz. Analizará el modelo de Deming para poder asegurar los planes de Continuidad en el negocio y administración en la recuperación ante desastres, alineándolos a los estándares internacionales (Cobit, ISO 27005, ITIL).

Por el lado de la oferta, se da un tratamiento especial, en cuanto a la emisión de valores, a las pequeñas, medianas y microempresas-Pymes para que puedan acceder a través del mercado de valores al financiamiento. Las empresas públicas podrían participar en el mercado, a través de emisiones, como lo plantea el nuevo proyecto de "Ley de Empresas Públicas".[4]

En este ámbito el sistema de administración de riesgos integral de Tecnología de Información, aumentará la confianza y seguridad del inversionista, con el propósito de incentivar la innovación tecnológica y la competencia; el establecer una plataforma tecnológica integrada para el mercado de

[4] E con Luis Rosero M, 2009, www.bce.fin.ec/documentos/PublicacionesNotas/.../BPrensa149.pdf).

valores con un solo mercado, cumpliendo los estándares internacionales. Un tema fundamental es la obligación de todos los participantes del mercado de valores de aplicar las prácticas de buen gobierno corporativo de tecnología de información a fin de establecer las reglas del juego entre los accionistas, administradores, y comisarios, de manera que no existan perjuicios entre las partes que constituyen la empresa y se defienda al accionista minoritario.

1.5.- JUSTIFICACIÓN

En las empresas participantes del mercado de valores, la tecnología soporta los procesos de negocio por lo cual es necesario realizar una eficiente administración de riesgos de T.I. para conocer si nuestra infraestructura tecnológica que sobrelleva los procesos de negocio reúne los requisitos mínimos necesarios para poder seguir prestando el servicio de fundamento a la institución.

Actualmente no hay estudios que comprueben que la práctica de gestión de riesgos en T.I. se está desarrollando o llevando a cabo en las empresas, es por esto que he decidido realizar esta investigación con propósito de determinar cuál es la importancia de la función de la administración de riesgos en T.I. y promover ésta función dentro de dichas empresas.

Es importante subrayar que un modelo de Administración de riesgos asociados a las T.I. es independiente de que la empresa siga o no funcionando de la misma forma, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. Considerando que por su relevancia debería tener carácter de ejecutivo.

Aunque actualmente ya existen marcos de mejores prácticas a este respecto, dichos marcos fueron desarrollados basados en grandes economías, es decir, soportados en empresas cuyas características les permiten realizar grandes inversiones en cuanto a la adquisición de infraestructura y tecnologías de información se refiere y por ende estos marcos no pueden ser aplicados de la misma forma para la realización de Administración de riesgos asociados a la T.I.

Debido al desconocimiento de las tendencias en las T.I. así como las metodologías de gestión de riesgos en las T.I. surge en las empresas la necesidad de contar con modelos (actualmente inexistentes) que sirvan de guía y recomienden una mejor gestión de la administración de los controles, procesos en el manejo de la información su confidencialidad, disponibilidad e integridad basada en las necesidades y objetivos de la organización que contenga elementos de análisis de verificación y de exposición de debilidades y disfunciones, y que por ende les permita alcanzar sus objetivos y competir en esta nueva era llamada globalización. Al desarrollar un modelo que sirva de guía a las empresas, permitirá emitir sugerencias y planes de acción para eliminar las disfunciones y debilidades ya mencionados (recomendaciones).

Del anterior análisis, evaluación, diagnóstico y modelo a conseguir, entonces en el proyecto de tesis, se propone una Metodología que permita obtener un sistema o medio ambiente a través de la utilización de objetivos de control y sus actividades para crear un medio de seguridad de la información, el activo más valioso de toda empresa, después del recurso humano la misma que es operada por las Tecnologías de Información para la empresa.

CAPÍTULO II.- GENERALIDADES Y SU COMPARACIÓN CON EL MERCADO DE VALORES EN MÉXICO

2.1.- ANTECEDENTES DEL MERCADO DE VALORES EN EL ECUADOR

Para poder realizar una clara exposición del trabajo es imprescindible partir de la existencia de las bolsas de valores en el Ecuador, en realidad tiene un origen muy remoto. Se podría aventurar que surgen cuando los antiguos mercaderes se reunían en algún lugar conocido con el propósito de comprar o vender sus productos primarios. A medida que pasó el tiempo fue ampliándose el espectro de los bienes objeto de intercambio, hasta llegar finalmente a la producción y negociación de productos más sofisticados y complejos como son valores representativos de derechos económicos, sean patrimoniales o crediticios.

En ese proceso se detallan los hechos y fechas más relevantes que conforman la historia jurídica del sistema bursátil.

- Se creó la Comisión Nacional de Valores en Julio 4 de 1955, en el Decreto Ejecutivo No. 34.
- Se expidió la Ley de la Comisión de Valores - Corporación Financiera Nacional sustituyendo a la Comisión Nacional de Valores, Agosto 11 de 1964.
- Se expidió la Ley No.111 que faculta el establecimiento de bolsas de valores, compañías anónimas, otorgando facultad a la Comisión de Valores - Corporación Financiera Nacional para fundar y promover la constitución de la Bolsa de Valores de Quito C.A, en, Marzo 26 de 1969.
- Se autorizó el establecimiento de las Bolsas de Valores en Quito y Guayaquil, Mayo 30 de 1969,
- Se otorgó Escritura de Constitución de la Bolsa de Valores de Quito C. A, Agosto 25 de 1969.
- Se expidió la primera Ley de Mercado de Valores, en donde se establece que las Bolsas de Valores deben ser corporaciones civiles y dispone la transformación jurídica de las compañías anónimas, Mayo 28 de 1993.
- Se realizó la transformación jurídica de la Bolsa de Valores de Quito C.A. a la Corporación Civil Bolsa de Valores de Quito, Mayo 31 de 1994.

La Bolsa de Valores de Quito (capital de la República del Ecuador), busca adecuarse positivamente a los requerimientos y exigencias de un mercado dinámico, eficiente y especializado, estableciendo como visión fundamental "ser la institución natural del mercado de Valores", y como Misión "ofrecer el medio eficaz para lograr los mejores precios de los títulos valores al más bajo costo y en el menor tiempo de transacción" . [5]

[5] Fundación Ecuador Libre, disponible en: http://www.ecuadorlibre.com/index.php?option=com_content&view=article&id=415:cap-no163-qel-mercado-de-valores-ecuatorianoq&catid=3:capsula-de-entorno-economico&Itemid=12

2.1.1. CÓMO PARTICIPA EN LOS MERCADOS INTERNACIONALES EL MERCADO DE VALORES ECUATORIANO

Actualmente con la Ley de Mercado de Valores vigente la participación internacional es mínima, este mercado está poco desarrollado en el país, tal es así que en el 2007, las operaciones transadas en las bolsas de valores representaron solo el 8% del PIB, y en 2008 alcanzaron el 10% del PIB, cuando en otros países de América Latina como es el caso de México, Chile, Brasil y Colombia bordean el 50% del PIB. Otros factores que afectan la participación internacional es que existen dos mercados uno por cada bolsa de valores (liquidez segmentada) y geográficamente limitada, no existe mercado secundario, falta curvas de rendimiento, escasa desmaterialización, falta de cultura bursátil y finalmente la existencia de un regulador y supervisor débil. Por estas razones fundamentales el gobierno ecuatoriano busca fortalecer, dinamizar y desarrollar el mercado de valores a través de una Reforma Integral, cuyo primer paso es el Proyecto de Ley del Mercado de Valores. En la actualidad el mayor inversionista en el Mercado de Valores de Ecuador, es el Instituto Ecuatoriano de Seguridad Social (IESS), con el 61,34% de participación en el mismo. Con la nueva Ley se establece nuevas alternativas de financiamiento y oportunidades para el sector productivo interno, moviliza el ahorro a la inversión(al momento de comprar acciones una persona natural o jurídica, nacional o internacional traspasa sus ahorros a las empresas); transparenta el mercado porque la información es pública para inversionistas y empresas, genera estímulos para el desarrollo empresarial, seguridad y confianza en el mercado internacional.

2.2. BREVE DIAGNÓSTICO DEL FUNCIONAMIENTO ACTUAL DEL MERCADO DE VALORES EN EL ECUADOR

El mercado de valores canaliza los recursos financieros hacía las actividades productivas a través de la negociación de valores. En este sentido, el mercado de valores comprende aquel espacio económico donde se reúnen oferentes (emisores) y demandantes (inversionistas) de valores. A su vez, el mercado de valores cumple la función de captar recursos financieros a través de la compra y venta de instrumentos financieros, con el objetivo de financiar capital de trabajo de manera directa y a costos reducidos.

En Ecuador, las principales instituciones encargadas de regular el mercado de valores son: El Consejo Nacional de Valores y la Superintendencia de Compañías. De acuerdo a la Ley de Mercado de Valores, El Consejo Nacional de Valores constituye el órgano rector y encargado de establecer la política general del mercado de valores. Mientras que la Superintendencia de Compañías, es la encargada de ejecutar las políticas dispuestas por el Consejo Nacional de Valores y regular las actividades llevadas a cabo dentro del mercado de valores. Adicionalmente se tiene al registro de mercado de valores, el cual forma parte de la Superintendencia de compañías como el organismo encargado de registrar la información pública de los participantes del mercado.

Por otro lado, se tiene a la bolsa de valores como el espacio físico donde acuden los distintos actores del mercado a realizar sus transacciones de compra o venta de valores. Este proceso de negociación de valores, se realiza a través de intermediarios (casa de valores) las cuales son las encargadas de vender títulos valores emitidos por sus clientes (emisores) o comprar títulos valores por encargo de los inversionistas. Actualmente, en Ecuador existen dos bolsas de valores: Bolsa de Valores de Guayaquil (BVG) y Bolsa de Valores de Quito (BVQ). Dentro de las cuales constan registradas al año 2009 un total de 34 casas de valores (21 en Quito y 13 en Guayaquil).

En cuanto a los tipos de títulos de valores estos pueden ser de renta fija o variable. Los títulos de renta fija, son aquellos documentos a través de los cuales el inversionista percibe una cantidad conocida en cada período u otorga el derecho a percibir un interés fijo (Bonos, Certificado de depósito, entre otros). Mientras, que los títulos de renta variable son aquellos que incluyen un derecho de propiedad sobre el patrimonio de una empresa, el cual generará un flujo de dinero incierto que dependerá del desempeño de la empresa y los beneficios que esta obtenga (acciones). De acuerdo a cifras oficiales al 2009, las transacciones bursátiles de títulos valores fue de USD 6,426 millones a nivel nacional (USD 5,070 millones renta fija y USD 1,355 millones renta variable) con una participación del 27% sector público y 73% sector privado.

El monto de papeles de Renta Variable fue de 49 millones 551 mil dólares, mientras que el de Renta Fija alcanzó el 97.22 por ciento, es decir, 1730 mil 758 millones de dólares, dentro del período de enero a abril del 2010.

En el mismo periodo de Enero a Abril del presente año 2010, se colocaron emisiones de obligaciones por 92 millones 821 mil 900 dólares y que las llamadas titularizaciones fueron de 182 millones 938 mil 325 dólares.

En Abril 2010, la composición del mercado nacional mostró una mayor participación de la Bolsa de Valores de Guayaquil con el 51.33 por ciento, mientras que la de Quito negoció el 48.67 por ciento del total nacional.[6] Lo que constituye una fuente directa de financiamiento y una interesante opción de rentabilidad para los inversionistas.

Los fondos de inversión existentes en el Ecuador concentran sus inversiones en papeles del sector financiero como certificados de depósito, pólizas de acumulación, titularizaciones entre otros. Lo que da como resultado que los fondos de inversión sean una fuente de fondeo más para las instituciones financieras del país. Es decir, las instituciones financieras del país se benefician del mercado bursátil mediante la obtención de fondos que posteriormente prestan y de los cuales obtienen beneficios gracias a la intermediación financiera.

Pero el objetivo principal del mercado bursátil no es crear más fondos para las instituciones financieras y de esta forma promover la intermediación financiera, sino más bien, busca fomentar la intermediación bursátil que consiste en vincular a los inversionistas con los productores sin la intervención de instituciones financieras; de modo que los productores obtengan créditos más baratos y los inversionistas rendimientos más altos, además de permitir la participación de pequeños y medianos inversionistas dentro de este proceso.

2.2.1.- PROBLEMAS A LOS QUE SE ENFRENTA EL MERCADO DE VALORES ECUATORIANO

Dentro de los problemas que pueden afectar al mercado de valores figuran: los problemas coyunturales (inestabilidad política, jurídica o volatilidad de mercados internacionales) y los estructurales (regulación del mercado, incentivos tributarios, productos financieros). De esta manera, se tiene que a pesar de los problemas coyunturales en el último año, el país obtuvo un incremento de sus transacciones bursátiles en un 20% (USD 1273 millones), pasando de USD 5,153 millones en el 2008 a USD 6,426 millones en el 2009[5]. No obstante, problemas como la reducción de incentivos tributarios resultado de la última reforma a la ley de régimen tributario y el constante incremento de la carga tributaria a los distintos sectores de la economía, podrían mermar el desarrollo del mercado de valores[7]

Actualmente el mercado de valores ecuatoriano no se ha desarrollado eficientemente debido, principalmente, a la falta de cultura bursátil (problema de tipo estructural); es decir: por un lado los individuos con recursos excedentes se convierten en ahorristas pues el sistema bancario ha canalizado la información de tal forma que sean ellos los únicos receptores de dichos recursos, evitando así que éstos sean invertidos en el mercado de valores.

[6] Revista Financiera, Gestiopolis, agosto 2002, disponible en,http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/bolsasmundo.htm
[7] Fundación Ecuador Libre, julio 2009, disponible en: http://www.ecuadorlibre.com/index.php?option=com_content&view=article&id=415:cap-no163-qel-mercado-de-valores-ecuatorianoq&catid=3:capsula-de-entorno-economico&Itemid=12

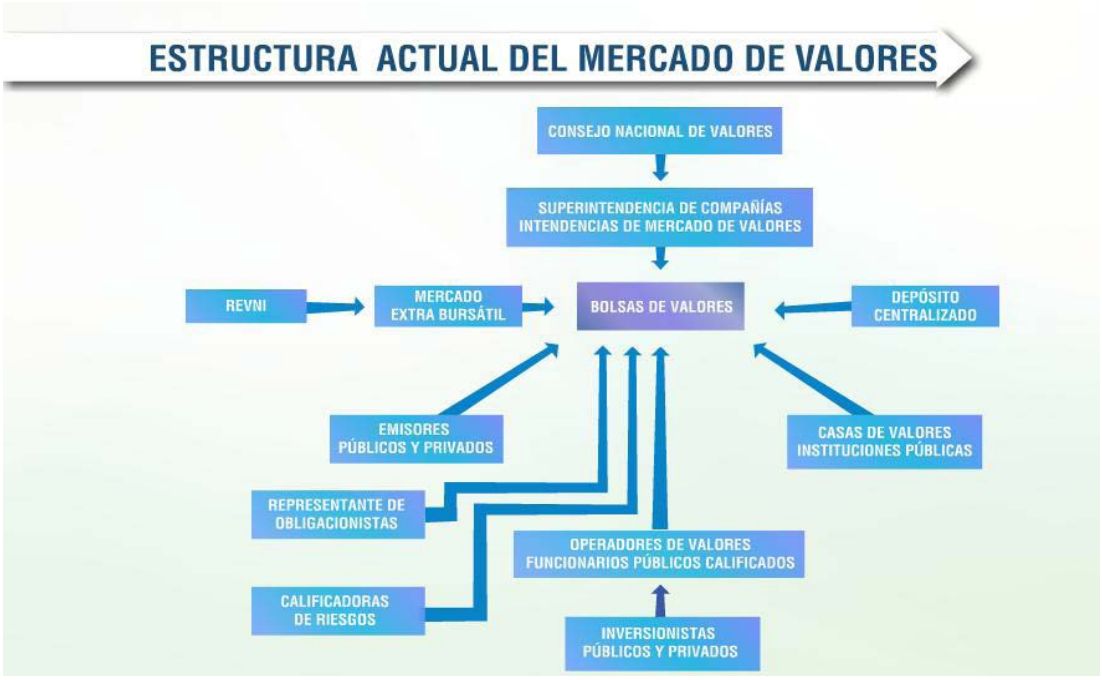
Por otro lado, está la falta de promoción del mercado de valores sobre los beneficios que pueden recibir los individuos al invertir sus recursos en la adquisición de acciones, bonos y demás títulos valores; cabe resaltar que dicha promoción también debe ser dirigida hacia las empresas; la mayor parte de las empresas que funcionan en el Ecuador son de patrimonios familiares con capitales cerrados al mercado de valores pues no conocen los beneficios que conllevan inscribirse y participar en el mercado.

A pesar de que son varios los trabajos que se han realizado sobre los factores que afectan al crecimiento y desarrollo del mercado de valores, en la mayoría de ellos se cita como factor fundamental la intervención del Gobierno en el establecimiento de incentivos tributarios para la formación de una cultura bursátil que propicie y garantice la realización de transacciones en el mercado de valores.

El Mercado de Valores ecuatoriano en la actualidad no se encuentra lo suficientemente desarrollado en comparación con los mercados de los demás países de la región; por lo que es necesario analizar mecanismos que fomenten su desarrollo; en el caso ecuatoriano, es evidente la necesidad de restablecer los incentivos tributarios que se estipularon en la primera Ley del mercado de valores; así como también, la inclusión de nuevas reformas tributarias que incentiven tanto a los inversionista para que canalicen sus recursos hacia la inversión productiva; y a las empresas para que se inscriban en el mercado de valores favoreciendo al crecimiento de éste.

2.2.2 ESTRUCTURA ACTUAL DEL MERCADO DE VALORES ECUATORIANO[8]

ILUSTRACIÓN 2 ESTRUCTURA ACTUAL DEL MERCADO DE VALORES



[8] Superintendencia de Compañías en Ecuador- Guía del Mercado de Valores 2010

Realizando una breve descripción de la **ilustración No.2,** el mercado de valores en el Ecuador resaltamos lo siguiente: De acuerdo a Ley de Mercado de Valores de 23 de Julio de 1998, el Consejo Nacional de Valores es el Organismo encargado de establecer la política general del mercado de valores y de regular su actividad. Está adscrito a la a la Superintendencia de Compañías e integrado por siete miembros, cuatro del sector público y tres del sector privado.[9]

La Superintendencia de Compañías es el organismo técnico y autónomo que vigila y controla la organización, actividades, funcionamiento, disolución y liquidación de las compañías, en las Además, según el artículo 10 de la Ley del Mercado de Valores, tiene entre otras las siguientes atribuciones:

- Ejecutar la política general del mercado de valores dictada por el C.N.V.
- Inspeccionar, en cualquier tiempo, a las compañías, entidades y demás personas que intervengan en el mercado de valores.
- Investigar las denuncias e infracciones a la Ley de Mercados de Valores, sus reglamentos y regulaciones de las instituciones reguladas por esta Ley, y sancionar, en primera instancia, las infracciones a la Ley, reglamentos, resoluciones y demás normas secundarias.
- Requerir y suministrar la información referente a la actividad de las personas naturales o jurídicas bajo su control.

Autorizar el funcionamiento en el mercado de valores de Bolsas de Valores, Casas de Valores, Compañías Calificadoras de Riesgos, Depósitos Centralizados de Compensación y Liquidación de Valores, Sociedades Administradoras de Fondos y Fideicomisos, Auditores Externos y demás entidades que intervengan en el mercado.

2.2.3.-CLASIFICACIÓN DEL MERCADO DE VALORES

El Mercado de Valores está compuesto por los siguientes segmentos: [10]

- PÚBLICO, son las negociaciones que se realizan con la intermediación de una casa de valores autorizada.
- PRIVADO, son las negociaciones que se realizan en forma directa entre comprador y vendedor, sin la intervención de una casa de valores.
- PRIMARIO, es aquel en el cual se realiza la primera venta o colocación de valores que hace el emisor con el fin de obtener directamente los recursos.
- SECUNDARIO, comprende las negociaciones posteriores a la primera colocación de valores.

2.2.4.- ENTIDADES DE CONTROL DEL MERCADO DE VALORES ECUADOR[11]

- CONSEJO NACIONAL DE VALORES es el órgano adscrito a la SUPERINTENDENCIA DE COMPANIAS que establece la política general del mercado de valores y regula su funcionamiento.

[9] Autor: Bolívar de Jesús jumbo El entorno financiero y los mercados, 08-2002
[10] Revista Financiera, agosto 2002,http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/bolsasmundo.htm
[11] Revista Financiera, agosto 2002,http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/bolsasmundo.htm

- SUPERINTENDENCIA DE COMPANIAS es la institución que ejecuta la política general del mercado de valores y controla a los participantes del mercado.
- BOLSAS DE VALORES a través de su facultad de autorregulación pueden dictar sus reglamentos y demás normas internas de aplicación general para todos sus partícipes, así como, ejercer el control de sus miembros e imponer las sanciones dentro del ámbito de su competencia.

2.2.5.-PARTICIPANTES DEL MERCADO DE VALORES EN EL ECUADOR [12]

- EMISORES, son compañías públicas, privadas o instituciones del sector público que financian sus actividades mediante la emisión y colocación de valores, a través del mercado de valores.
- INVERSIONISTAS, son aquellas personas naturales o jurídicas que disponen de recursos económicos y los destinan a la compra de valores, con el objeto de lograr una rentabilidad adecuada en función del riesgo adquirido. Para participar en el mercado de valores no se requiere de montos mínimos de inversión.
- BOLSAS DE VALORES, son corporaciones civiles sin fines de lucro que tienen por objeto brindar los servicios y mecanismos necesarios para la negociación de valores en condiciones de equidad, transparencia, seguridad y precio justo.
- CASAS DE VALORES son compañías anónimas autorizadas, miembros de las bolsas de valores cuya principal función es la intermediación de valores, además de asesorar en materia de inversiones, ayudar a estructurar emisiones y servir de agente colocador de las emisiones primarias.
- DEPOSITO CENTRALIZADO DE COMPENSACIÓN Y LIQUIDACIÓN DE VALORES, es una compañía anónima que se encarga de proveer servicios de depósito, custodia, conservación, liquidación y registro de transferencia de los valores. Opera también como cámara de compensación.
- CALIFICADORAS DE RIESGO, son sociedades anónimas o de responsabilidad limitada, independientes, que tienen por objeto la calificación de emisores y valores.
- ADMINISTRADORAS DE FONDOS Y FIDEICOMISOS son compañías anónimas que administran fondos de inversión y negocios fiduciarios.

2.2.6.-MECANISMOS DEL MERCADO DE VALORES EN EL ECUADOR.-

- REGISTRO DEL MERCADO DE VALORES, es el lugar en el que se inscriben los valores, emisores, casas de valores y demás participes del mercado, los mismos que deberán proveer información suficiente y actualizada.
- OFERTA PUBLICA, es la propuesta dirigida al público en general, o a sectores específicos, con el propósito de negociar valores en el mercado.
- CALIFICACION DE RIESGO, es la actividad que realizan las calificadoras de riesgo con el objeto de dar a conocer al mercado y al público su opinión sobre la solvencia y probabilidad de pago que tiene un emisor de valores.
- RUEDA DE BOLSA, es la reunión o sistema de interconexión de operadores de valores que, en representación de sus respectivas casas de valores, realizan transacciones con valores inscritos en el registro de mercado de valores y en bolsa.
- Existen dos clases de Ruedas de Bolsa:

[12] Revista Financiera, agosto 2002,disponibleen,http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/bolsasmundo.htm

- RUEDA DE PISO, es la concurrencia física de operadores de valores, con el objeto de ofertar y demandar instrumentos en el corro o lugar físico que pone a disposición para tal efecto la bolsa de valores.
- RUEDA ELECTRÓNICA, es el sistema de interconexión en el que las ofertas, demandas, calces y cierres de operaciones se efectúan a través de una red de computadores, de propiedad de la bolsa o contratada por ella[13].

2.3. ANÁLISIS DEL MERCADO DE VALORES EN MÉXICO

La Bolsa Mexicana de Valores (BMV), foro en el que se llevan a cabo las operaciones del mercado de valores organizado en México, siendo su objeto el facilitar las transacciones con valores

Y procurar el desarrollo del mercado, fomentar su expansión y competitividad, a través de las siguientes funciones:

- Establecer los locales, instalaciones y mecanismos que faciliten las relaciones y operaciones entre la oferta y demanda de valores, títulos de crédito y demás documentos inscritos en el Registro Nacional de Valores (RNV), así como prestar los servicios necesarios para la realización de los procesos de emisión, colocación en intercambio de los referidos valores;
- Proporcionar, mantener a disposición del público y hacer publicaciones sobre la información relativa a los valores inscritos en la BMV y los listados en el Sistema Internacional de Cotizaciones de la propia Bolsa, sobre sus emisores y las operaciones que en ella se realicen;
- Establecer las medidas necesarias para que las operaciones que se realicen en la BMV por las casas de bolsa, se sujeten a las disposiciones que les sean aplicables;
- Expedir normas que establezcan estándares y esquemas operativos y de conducta que promuevan prácticas justas y equitativas en el mercado de valores, así como vigilar su observancia e imponer medidas disciplinarias y correctivas por su incumplimiento, obligatorias para las casas de bolsa y emisoras con valores inscritos en la BMV.

Las empresas que requieren recursos (dinero) para financiar su operación o proyectos de expansión, pueden obtenerlo a través del mercado bursátil, mediante la emisión de valores (**acciones**, **obligaciones**, **papel comercial**, etc.) que son puestos a disposición de los **inversionistas** (colocados) e intercambiados (comprados y vendidos) en la BMV, en un mercado transparente de libre competencia y con igualdad de oportunidades para todos sus participantes.

Dentro de este análisis la investigación se centrará en el funcionamiento de la entidad INDEVAL, del Grupo BMV.[14]

2.3.1. ¿QUÉ ES EL INDEVAL?

Indeval es la institución privada que cuenta con autorización de acuerdo a la Ley, para operar como Depósito Central de Valores, que ofrece al sistema financiero mexicano de guarda, custodia, administración, compensación y liquidación de valores, en un ámbito de máxima confianza y seguridad.

[13] Autor: Julio Baldeón, año 1998, Monografías Trabajos en web
[14] Bolsa Mexicana de Valores- www.bmv.com.mx

En otras palabras todos los valores que se compran o venden en el mercado financiero, casas de bolsa, bancos, operadoras, distribuidoras de fondos etc. son guardados y administrados únicamente en el Indeval.

Operaciones nacionales: guarda física de los valores y/o su registro electrónico en instituciones autorizada para este fin; ejercicios de derechos en efectivo, en especie y mixtos. Transferencia electrónica de valores y efectivo. Compensación de operaciones y liquidación DVP y de operaciones (diversos plazos) para el Mercado de Dinero (directo y reporto) y Mercado de Capitales (operaciones pactadas en la Bolsa).Operaciones internacionales; transferencia electrónica de valores, de efectivo compensación de operaciones y liquidación[15].

2.3.2.-PRINCIPALES PROCESOS DE NEGOCIO DEL INDEVAL.-

Desde el punto de vista transaccional (compra/venta de títulos), los "mercados de valores" tienen tres procesos o funciones de soporte central para sus operaciones: la función de Depósito, la función de Liquidación y a veces una función de Contraparte. En México, la función de Depósito y Sistema de Liquidación de Valores se encuentra en el Indeval (Depósito Central de Valores – DCV dentro del cual se encuentra el Sistema de Liquidación de Valores – SLV) y la función de Contraparte en la Contraparte Central de Valores – CCV. **Ilustración No.3**

En cuanto a la concertación o "trading", las Bolsas apoyan a los intermediarios financieros ofreciendo un lugar centralizado donde negociar títulos aunque también existen otros "mecanismos de negociación" conocidos como "bróker" que cumplen funciones similares. La concertación también se puede hacer sin la intervención de los anteriores mecanismos, directamente entre intermediarios (bancos o casas de bolsa) en operaciones llamadas sobre-el-mostrador (OTC, "Over-The-Counter")[16]. De cualquier forma, las operaciones deben ser liquidadas en algún sistema de liquidación de valores (SLV) y registradas en las cuentas del depósito central de valores (DCV)[17].

ILUSTRACIÓN 3 INSTRUMENTOS Y OPERACIONES DEL INDEVAL S.A.

[15] http://www.oem.com.mx/esto/notas/n911892.htm

[16] Las acciones rara vez se pueden negociar fuera de una bolsa centralizada.

[17] En México, el depósito y el sistema de liquidación no son empresas separadas. El Sistema de Liquidación de Valores (SLV) no puede operar sin tomar control de las cuentas del Depósito Central de Valores (DCV) y necesita toda la información detallada de éstas

2.3.2. EJES ESTRATÉGICOS DEL INDEVAL Y CCV.

De acuerdo al siguiente esquema podemos observar como los ejes estratégicos afectan de manera directa a los objetivos y estrategias del INDEVAL, analicemos el siguiente cuadro: **(véase Ilustración No.4)**

ILUSTRACIÓN 4 ALINEAMIENTO DE LOS EJES ESTRATÉGICOS DEL GRUPO BMV CON LOS OBJETIVOS ESTRATÉGICOS DE INDEVAL Y CCV.

ALINEAMIENTO DE LOS EJES ESTRATÉGICOS DEL GRUPO BMV CON LOS OBJETIVOS ESTRATÉGICOS INDEVAL Y CCV

EJES ESTRATÉGICOS	OBJETIVOS ESTRATÉGICOS Y ESTRATEGIAS INDEVAL	OBJETIVOS ESTRATÉGICOS Y ESTRATEGIAS CCV
Eficiencia Operativa	▫ Brindar los servicios, enfatizando la confianza y la seguridad en la operación de los clientes	▫ Brindar servicios en un ámbito de máxima confianza Las necesidades de los clientes deben ser satisfechas mediante servicios transparentes y eficientes, con altos estándares de calidad
Promoción de los mercados	▫ Adopción de tecnologías internacionales para promover la conexión del mercado mexicano con el exterior	▫ Brindar servicios en un ámbito mitigación de riesgos mediante la adopción de garantías apropiadas.
Robustecer Tecnología	▫ Indeval seguirá apoyandose en la solidez fiancniera, en tecnología apropiada, en la dopción y desarrollo de las mejores prácticas de la industria y en su capital humano	▫ Fortalecer la automatización de procesos mediante innovación en TI
Innovar productos y servicios	▫ Incursión en nuevos mercados y generación de nuevos productos	▫ Incursión en nuevos mercados y generación de nuevos productos

Análisis de la ilustración No.4.-

En el cuadro podemos destacar que los ejes estratégicos en los que se basan las instituciones: INDEVAL y CCV, son cuatro: Eficiencia operativa, Promoción de los mercados, Robustecer la Tecnología e Innovar productos y servicios.

Los objetivos estratégicos en que coinciden el INDEVAL y CCV son: brindar los servicios enfatizando la seguridad y confianza en las operaciones de los clientes, adoptando tecnologías internacionales promoviendo de esta manera el mercado mexicano con el exterior, y siendo sus principales fortalezas la solidez financiera y aplicando las mejores prácticas de la industria y en su capital humano. Sus metas son creación de nuevos productos e incursión en nuevos mercados[18].

2.3.3.- PROCESO OPERATIVO DEL INDEVAL[19]

El proceso operativo de INDEVAL se basa en tres áreas:

- Administración de Valores
- Custodia
- Mercado de dinero

ADMINISTRACIÓN DE VALORES

Este servicio se encarga de administrar todos los instrumentos financieros almacenados en la bóveda física y en una bóveda electrónica que se conoce como Bóveda Ampliada.

Entre las principales funciones del Área de administración de Valores se encuentran:

- Ejercicios de derechos en efectivo: dividendos en efectivo, pago de intereses y amortizaciones.
- Ejercicios de derechos en especie: capitalizaciones, canjes, conversiones y Split.
- Ejercicios de derechos mixtos: suscripciones.

CUSTODIA

- Este servicio consiste en la guarda física de los valores y/o su registro electrónico en la institución autorizada para este fin (S.D.Indeval), la cual asume la responsabilidad por los valores en depósito.
- S.D. Indeval presta el servicio de depósito y custodia bajo las siguientes características
- Depósito y retiro físico de documentos de las bóvedas de la institución, utilizando el endoso en administración como figura legal.
- Inmovilización de documentos.
- Custodia centralizada de todos los valores inscritos en el Registro Nacional de Valores e Intermediarios (títulos bancarios, títulos gubernamentales, títulos de deuda privada y acciones) que son negociados en mercados financieros, ya sea en la BMV o fuera de ella.

[18] www.indeval.com
[19] Información obtenida de la página web de Indeval: www.indeval.com.mx

- Desmaterialización a través del programa permanente de reducción de documentos, que promueve la emisión del título único para nuevas emisiones y la conversión a macro título de los documentos que amparan emisiones ya depositadas.
- 2 bóvedas: una en México, D.F. y otra en Monterrey, N.L.

MERCADO DE DINERO

- Las instituciones emisoras colocan para su operación, emisiones de títulos bancarios a través de Indeval, tales como Pagares con Rendimiento Liquidable al Vencimiento, Aceptaciones Bancarias, Bonos Bancarios y CEDES, ya sea que den de alta una nueva emisión de éstos o que se requiera incrementar una ya existente.
- El área de Mercado de Dinero se encarga de liquidar las obligaciones pendientes del Mercado de Deuda para cada participante. Concluye una operación mediante la transferencia de Títulos y Dinero para cada uno de los participantes.- clausulado de la emisión.
- Durante el día la Subdirección de Liquidaciones y Mercado de Dinero realiza monitoreo de la operación vía sistema y telefónicos, para estar al pendiente de que la marcha de operaciones y líneas de usuarios se encuentran en perfecto estado.

Desde un punto de vista de Tecnologías de Información, el INDEVAL puede definirse como un sistema de procesamiento de información, por lo que puede quedar perfectamente definido si se especifican las reglas que transforman las entradas al sistema y generan los cambios necesarios en la base de datos del sistema.

En el sistema de información del INDEVAL se identifican cuatro grandes clases de negocio:

- Participantes;
- Instrumentos;
- Cuentas;
- Instrucciones.

Participantes.-

Parte interesada stakeholders en un sistema de pago, son las partes cuyos intereses se ven afectados por las operaciones del sistema.

Participante directo, direct participant, un participante en un Sistema Interbancario de Transferencia de Fondos (SITF) que es responsable ante el agente liquidador (o ante los demás participantes directos) de la liquidación de sus propios pagos, los de sus clientes y los de los participantes indirectos en cuyo nombre está efectuando la liquidación.

Participante directo del mercado, direct market participant, un intermediario o un miembro de un mercado que ejecuta directamente una orden.

Participante indirecto del mercado, indirect market participant, un participante del mercado que utiliza a un intermediario para ejecutar las negociaciones en su nombre. Generalmente los clientes institucionales y transfronterizos son participantes indirectos del mercado.

P**articipante /miembro, participant/member,** una de las partes que participa en un sistema de transferencia. Este término genérico se refiere a una institución identificada mediante un sistema de transferencia (Vg., por un número de identificación bancario) y a la que se le permite enviar órdenes de pago directamente al sistema o a una institución que se encuentra directamente obligada por las normas que rigen el sistema de transferencia.

Participante /miembro directo/direct participant/ member, el término se refiere generalmente a participantes en un sistema de transferencia de fondos o de valores que intercambian directamente órdenes de transferencia con otros participantes del sistema. En algunos sistemas, los participantes directos también intercambian órdenes en nombre de participantes indirectos.

Dependiendo del sistema, los participantes directos pueden ser también participantes liquidadores.

En la Unión Europea, este término tiene un significado específico: se refiere a los participantes en un sistema de transferencia que son responsables ante la institución liquidadora (o ante los demás participantes) de la liquidación de sus propios pagos, los de sus clientes y los de los participantes indirectos en cuyo nombre están efectuando la liquidación.

Participante /miembro/indirecto, indirect participant/member, se refiere a un sistema de transferencia de fondos o de valores en el cual existe un acuerdo de jerarquización de la participación. Los participantes indirectos se distinguen de los directos en que no pueden realizar algunas de las actividades propias del sistema que ejecutan los participantes directos (Vg., ingresar órdenes de transferencia, liquidar). Así, los participantes indirectos requieren de los servicios de los Participantes directos para que éstos ejecuten tales actividades en su nombre. En la Unión Europea, el término se refiere más específicamente a los participantes en un sistema de transferencia que son responsables sólo ante sus participantes directos de la liquidación de los pagos realizados en el sistema.

Participante /miembro liquidador /settling participant/member, en algunos países, un participante liquidador en un sistema de transferencia de fondos o de valores entrega y recibe éstos a / de otros participantes liquidadores por medio de una o más cuentas en la institución liquidadora, con el fin de liquidar transferencias de fondos o de valores en el sistema. Otros participantes requieren los servicios de un participante liquidador para poder liquidar sus posiciones. Actualmente en la Unión Europea los participantes directos son también, por definición, participantes liquidadores.

Participante remoto, remote participant, participante de un sistema de transferencia que no tiene ni su casa matriz ni ninguna de sus sucursales en el país donde se encuentra establecido el sistema de transferencia.

Instrumentos

Instrumento de pago, payment instrument, instrumento que permite al poseedor / usuario transferir fondos.

Instrumentos basados en tarjetas, card-based, products, instrumentos de dinero electrónico que proporcionan al cliente un dispositivo informático especializado portátil, generalmente una tarjeta de circuito integrado que contiene un chip microprocesador.

Instrumentos de acceso, Access products, instrumentos de pago que permiten a los clientes acceder a sus cuentas de depósitos y transferir los fondos depositados en éstas. Como ejemplos se

pueden incluir, entre otros, las transferencias electrónicas de fondos en el punto de venta y los servicios bancarios accesibles desde el hogar (home banking).

Cuentas

Cuenta ómnibus, ómnibus account, una cuenta única para los fondos o posiciones de múltiples partes. Por lo general, un miembro liquidador mantendrá una cuenta ómnibus para todos sus clientes en la cámara de compensación. En este caso, el miembro liquidador tiene la responsabilidad de mantener los registros contables de cada uno de los clientes.

Cuenta ómnibus de clientes, ómnibus customer account, una cuenta en la que se recogen los valores que mantiene un participante en nombre de todos (o al menos de varios de) sus clientes.

Cuenta propia o propietaria, propietary account, una cuenta en la que un participante mantiene sólo aquellos valores que mantiene por cuenta propia (en contraposición con aquellos valores que mantiene en nombre de sus clientes).

Cuentas de custodia para garantía, operational safe custody accounts, cuentas de valores administradas por el banco central en las cuales las instituciones de crédito pueden colocar valores que se consideran adecuados para garantizar las operaciones de banca central. Los valores que se mantienen en estas cuentas son finalmente depositados en la CDV a nombre del banco central nacional (BCN), de tal manera que la transferencia a una cuenta de custodia segura resulta en una transferencia entre el banco y la cuenta del BCN en la CDV. Los valores depositados en el BCN están por lo general pignorados a favor del BCN como garantía para préstamos a un día (que generan intereses) y para préstamos (que no generan intereses). También se pueden utilizar para operaciones de mercado abierto (repos) previa autorización general otorgada al BCN para adquirir valores.

Cuentas de registro de efectivo, cash memorándum accounts, registros que mantiene el sistema de liquidación de valores de los fondos que han vencido y que deben ser pagados o recibidos por los participantes junto con las liquidaciones de sus valores. Los registros sirven sólo para fines informativos y no representan derechos o responsabilidades legales entre los sistemas de liquidación de valores y sus participantes.

Instrucción

Orden de pago, payment message/ instruction, una orden o mensaje para transferir fondos (en forma de derechos monetarios girados sobre una parte) a la orden del beneficiario. La instrucción puede referirse a una transferencia de crédito o una transferencia de débito.

2.3.4.- SERVICIOS QUE BRINDA LA INSTITUCIÓN INDEVAL[20]

Indeval es la Institución privada que cuenta con autorización de acuerdo a la Ley, para operar como Depósito Central de Valores, proporcionando los siguientes servicios:

[20] Información obtenida en la página web: www.indeval.com.mx

Custodia y Administración de Valores

· Guarda física de los valores y/o su registro electrónico en instituciones autorizada para este fin.

· Depósito y retiro físico de documentos de las bóvedas de la institución; se tienen 2 bóvedas, una en México, D.F. y otra en Monterrey, N.L.

· Ejercicios de derechos en efectivo, en especie y mixtos

Operación Nacional

· Transferencia electrónica de valores

· Transferencia electrónica de efectivo

· Compensación de operaciones y liquidación DVP

· Liquidación de operaciones (diversos plazos) para el Mercado de Dinero (directo y reporto) y Mercado de Capitales (operaciones pactadas en la Bolsa)

· Administración de Colaterales

Operación internacional

· Liquidación de operaciones en mercados internacionales

· Administración de derechos patrimoniales de emisiones extranjeras

· Administración de impuestos sobre acciones estadounidenses

2.4.-COMPARACIÓN DEPÓSITO DE VALORES MÉXICO-ECUADOR

En México, el Instituto de Depósito de Valores (en adelante INDEVAL) es en la actualidad la única empresa autorizada en México para operar como depósito centralizado de valores. Es el custodio centralizado de todos los valores inscritos en el Registro Nacional de Valores que se negocian en los mercados financieros, ya sea en la Bolsa Mexicana de Valores (BMV) o fuera de ella. Además, el INDEVAL es el principal sistema de liquidación de valores (SLV) del sistema financiero mexicano: todas las operaciones del mercado de dinero (CETES, Bonos, títulos, deuda, etc.) se compensan y liquidan diariamente en el Indeval[21].

[21] En términos generales, se entiende por liquidación la conclusión de una operación mediante la transferencia definitiva de los valores y/o los recursos (fondos) entre dos partes, generalmente un comprador y el vendedor o el tras pasante y el receptor.

El INDEVAL provee un sistema de pagos que, junto con los sistemas de pagos del Banco de México, constituye el Sistema de Pagos de Alto Valor del país. En consecuencia, factores críticos para el buen funcionamiento del mercado financiero mexicano, como son la liquidez o la certeza en las transacciones, dependen de la eficiente administración de los recursos en el INDEVAL y de la confiabilidad y seguridad de sus sistemas.

El Depósito Central de Valores tiene funciones de guarda, custodia, administración, traspaso, compensación y liquidación de valores financieros. El INDEVAL es responsable de llevar a cabo esas labores para sus depositantes. La Contraparte Central de Valores tiene como principal objetivo mitigar el riesgo de contraparte que surge una vez concertada la operación en la Bolsa Mexicana de Valores (BMV), y hasta el momento de su liquidación. Hoy día y por la naturaleza de sus funciones, ambas entidades pueden llevar a cabo sus tareas de una manera altamente automatizada, en comparación de cómo se hacía en el pasado y por ello los sistemas aplicativos son parte primordial de sus activos.

Se muestra la interacción con los otros participantes del sistema financiero, en donde el Indeval actúa como el Depósito Central encargado de la guarda, custodia, administración, traspaso, compensación y liquidación de los valores financieros que emiten las sociedades.

Es el punto de partida que se quiere establecer para poder realizar las respectivas modificaciones adaptándolas a las necesidades del Ecuador e imitar procesos de entidades como es el caso del Indeval en este sentido la investigación se orienta para la conceptualización del sistema de administración de riesgos, el diseño de la red de relaciones que formarán el flujo de los registros de eventos.[22]

Estableciendo estos parámetros para comparación el estado ecuatoriano está realizando un diagnóstico para poder establecer la incidencia del Sistema Financiero en el Mercado de Valores ha sido demasiado elevado, y la mayor cantidad de valores tranzados en el mercado corresponden a emisiones financieras. **Ilustración No.5**

ILUSTRACIÓN 5 ESTRUCTURA PROPUESTA DEL MERCADO DE VALORES EN EL ECUADOR

23

[22] Entrevista con el Dr. Ramón Filorio T, Director de Gobierno Corporativo de Indeval.
[23] Banco Central del Ecuador, disponible en:http://www.bce.fin.ec/documentos/ElBancoCentral/proyectoLeyMercadoValores.pdf

2.4.1.- OBJETIVOS DE LA NUEVA LEY DE MERCADO DE VALORES EN PROYECTO EN EL ECUADOR

- Eliminar las trabas y distorsiones económicas, sociales y culturales que han impedido un normal desarrollo del mercado de valores en el Ecuador.
- Generar alternativas de financiamiento para el sector productivo en especial aquellos sectores excluidos por las normas y requerimientos existentes.
- Proyección internacional del mercado de valores ecuatoriano dentro de la lógica de la integración regional.
- Mejorar el esquema de Regulación y Control con la creación del Defensor del Inversionista
- Las emisiones se aclaran y refuerzan las garantías ofrecidas a los inversores y aumentando el control de las calificaciones (distorsiones en el mercado y riesgo camuflado).[24]

2.5.- ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA ADMINISTRACIÓN DE RIESGOS EN T.I. ECUADOR

Los riesgos de TI en el mercado de valores en el Ecuador son un componente del universo de riesgos a los que está sometida una organización. Considerando que existen riesgos a los que el mercado se enfrenta como son los riesgos estratégicos, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos y riesgos de cumplimiento. Los riesgos relacionados con TI se consideran un componente de riesgo operativo y se ajusta a las reglas del sector financiero en el marco de Basilea II, el cual es el segundo de los Acuerdos de Basilea, que consiste en recomendaciones sobre la legislación y regulación bancaria, es un estándar internacional que sirve de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos, publicado inicialmente en junio 2004, los 3 pilares en los que se fundamenta son :

1.- **El cálculo de los requisitos mínimos de capital**, constituye el núcleo del acuerdo, tiene como objetivo la calidad crediticia de los prestatarios (utilizando ratings externos o internos) y añada requisitos de capital por el riesgo operacional.

2.- **El proceso de supervisión de la gestión de los fondos propios**, los organismos supervisores nacionales, siendo el caso del Ecuador, la Superintendencia de Bancos, está facultado para incrementar el nivel de prudencia exigido a las instituciones financieras validando tanto los métodos estadísticos como la suficiencia de los niveles de fondos propios para hacer frente a una crisis económica, almacenando datos de información crediticia durante periodos largos, de 5 a 7 años , garantizando una adecuada auditoría. Se exige que la **alta dirección del banco** se involucre activamente en el control de riesgos y en la planificación futura de las necesidades de capital. Esta **autoevaluación** de las necesidades de capital debe ser discutida entre la alta dirección y el

[24] Ministerio de Coordinación de la Política Económica.- http://www.mcpe.gob.ec/MCPE/documentos/LMV_06_ENERO_2011_COMPLETA1.pdf

supervisor bancario. Como el banco es libre para elegir la metodología para su autoevaluación, se pueden considerar otros riesgos que no se contemplan en el cálculo regulatorio, tales como el riesgo de concentración y/o diversificación, el riesgo de liquidez, el riesgo reputacional, el riesgo de pensiones, etc.

3.- **La disciplina de mercado.-** El acuerdo estableció normas de transparencia y exigió la publicación periódica de información acerca de su exposición a los diferentes riesgos y la suficiencia de sus fondos propios. El objetivo es:

1. La generalización de las buenas prácticas bancarias y su homogeneización internacional.
2. La reconciliación de los puntos de vista financiero, contable y de la gestión del riesgo sobre la base de la información acumulada por las entidades.
3. La transparencia financiera a través de la homogeneización de los informes de riesgo publicados por los bancos.

Inicialmente la información debe incluir:

1. Descripción de la **gestión de riesgos**: objetivos, políticas, estructura, organización, alcance, políticas de cobertura y mitigación de riesgos.
2. **Aspectos técnicos** del cálculo del capital: diferencias en la consolidación financiera y regulatoria.
3. Descripción de la **gestión de capital**.
4. **Composición detallada de los elementos del capital** regulatorio disponible.
5. **Requerimientos de capital por cada tipo de riesgo**, indicando el método de cálculo utilizado.[25]

Sin embargo, incluso el riesgo estratégico de TI puede tener un componente financiero especialmente en las nuevas iniciativas empresariales. Por esta razón, no se describe los riesgos de TI con una dependencia jerárquica en una de las categorías de riesgo. El punto vulnerable del mercado es que no realizan la planificación, evaluación ni prevén los riesgos externos como son la dependencia de un número creciente de proveedores de servicios y una limitada disponibilidad de información fiable de control de riesgos. Para poder realizar un análisis más objetivo y crítico es necesario entender los componentes del tema de este proyecto de tesis. Los conceptos a estudiar serán:

- Conceptos de T.I. y características
- La importancia de las T.I. en la actualidad
- La gestión de las T.I. en las empresas participantes en el mercado de valores
- Ventajas y Desventajas del uso de las T.I. en las empresas

[25] Basilea II, disponible en: http://www.basilea2.com.ar/

2.5.1.- CONCEPTOS DE T.I. Y SUS CARACTERÍSTICAS[26]

Las **tecnologías de la información y la comunicación** (**TIC**, **TICS** o bien **NTIC** para Nuevas Tecnologías de la Información y de la Comunicación o **IT** para «Information Technology») agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet y telecomunicaciones.

Las TIC conforman el conjunto de recursos necesarios para manipular la información y particularmente los equipos de cómputo, programas informáticos y redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla. Actualmente se define a las tecnologías de información, según el autor Daniel Cohen como: "todas aquellas tecnologías que permitan y den soporte al diseño, desarrollo, implementación y operación en un negocio.

De los sistemas de información que conforman la infraestructura de la empresa que provee una plataforma en la cual se construye y operan los sistemas de información".

Según la asociación de la tecnología de información de América (ITAA) es "el estudio, diseño, implementación, soporte y dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras y sus componentes. Se ocupa del uso de los computadores y su software para convertir, almacenar, proteger, procesar, transmitir y recuperar la información".

La tecnología de información, según lo definido por el marco de referencia de ITIL (se entiende como "aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

Antes de continuar es preciso señalar el concepto de información de acuerdo a la norma ISO 27002:2005, ¨La información es un activo que, cómo otros activos de negocio importante, son esencial para el negocio de una organización y consecuentemente necesita estar protegido adecuadamente¨.

- La información puede existir en muchas formas:
- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida por correo, mensajería o por medios electrónicos
- Mostrada en video
- Hablada en una conversación

Sin importar en que medio o forma se encuentre la información, ésta debe ser protegida apropiadamente. La información para que se considere como tal debe de reunir las 3 propiedades básicas: Confidencialidad, Integridad y Disponibilidad.

La información nos permite ser eficientes todos los procesos internos de nuestra empresa, nos permite también conocer mejor a nuestra competencia así como el mercado por el que se compite. En general podemos conocer mejor el medio tanto interno como externo de nuestro negocio, para

[26]Wiki pedía: http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

así detectar nuestras debilidades y potencialidades, atacarlas, y lograr una ventaja competitiva con respecto a las demás empresas del ramo.

Por lo que las empresas más aún las financieras deben de crear sistemas que protejan a la empresa de los riesgos de seguridad de la información, que como bien dice el estándar de la ISO/IEC 27005:2008, "el potencial de que una cierta amenaza explote vulnerabilidades de un activo o grupo de activos y así cause daño a la organización¨.

Adicionalmente a esto, las Tecnologías de Información nos dan una ventaja competitiva, al reducir nuestros costos de operación, flexibilidad organizacional, rapidez en la toma de decisiones, respuesta hacia los requerimientos del cliente, información del mercado, competencia y entorno en general, además de manejar a las diferentes Unidades de Negocios como un todo, no importando su localidad física.

Hoy en día, el incremento en el uso del e-mail, el Internet, y el desarrollo de Intranets o redes de comunicaciones entre empresas, está acelerando el flujo de información en las empresas y negocios. Todos estos sistemas de transferencia y recuperación de información están basados en el uso de redes y computadoras personales unidas unas con otras y todas conectadas a una computadora central que permite a los usuarios compartir archivos e información digital de todo tipo.[27]

Características [28]

- **Inmaterialidad (Posibilidad de digitalización)**. Las TICS convierten la información, tradicionalmente sujeta a un medio físico, en inmaterial. Mediante la digitalización es posible almacenar grandes cantidades de información, en dispositivos físicos de pequeño tamaño (discos, CD, memorias USB, etc.).

  A su vez los usuarios pueden acceder a información ubicada en dispositivos electrónicos lejanos, que se transmite utilizando las redes de comunicación, de una forma transparente e inmaterial.
  Esta característica, ha venido a definir lo que se ha denominado como "realidad virtual", esto es, realidad no real. Mediante el uso de las Tics se están creando grupos de personas que interactúan según sus propios intereses, conformando comunidades o grupos virtuales.

- **Instantaneidad.** Podemos transmitir la información instantáneamente a lugares muy alejados físicamente, mediante las denominadas "autopistas de la información".

  Se han acuñado términos como ciberespacio, para definir el espacio virtual, no real, en el que se sitúa la información, al no asumir las características físicas del objeto utilizado para su almacenamiento, adquiriendo ese grado de inmediatez e inmaterialidad.

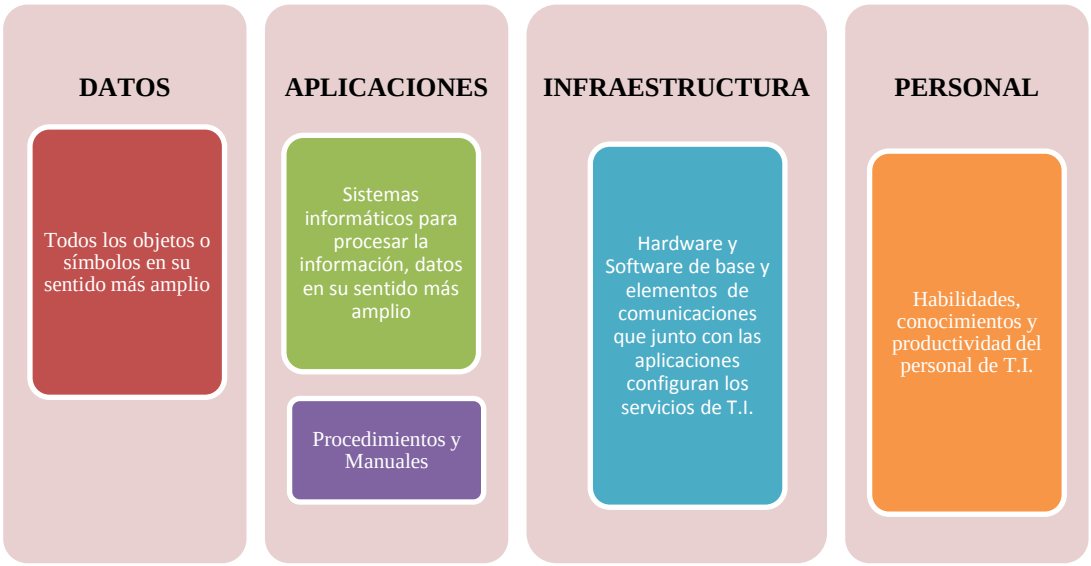
- **Aplicaciones Multimedia.** Las aplicaciones o programas multimedia han sido desarrollados como una interfaz amigable y sencilla de comunicación, para facilitar el acceso a las Tics de todos los usuarios. Una de las características más importantes de estos entornos es "La interactividad". Es posiblemente la característica más significativa. A diferencia de las tecnologías más clásicas (TV, radio) que permiten una interacción unidireccional, de un emisor a una masa de espectadores pasivos, el uso del ordenador interconectado mediante las redes digitales de comunicación, proporciona una

[27] http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/usoti.htm
[28] http://www.cibersociedad.net/archivo/articulo.php?art=218

comunicación bidireccional (sincrónica y asincrónica), persona- persona y persona- grupo. Se está produciendo, por tanto, un cambio hacia la comunicación entre personas y grupos que interactúan según sus intereses, conformando lo que se denomina "comunidades virtuales". El usuario de las TICS es por tanto, un sujeto activo, que envía sus propios mensajes y, lo más importante, toma las decisiones sobre el proceso a seguir: secuencia, ritmo, código, etc.

- Otra de las características más relevantes de las aplicaciones multimedia, y que mayor incidencia tienen sobre el sistema educativo, es la posibilidad de transmitir información a partir de diferentes medios (texto, imagen, sonido, animaciones, etc.). Por primera vez, en un mismo documento se pueden transmitir informaciones multi-sensoriales, desde un modelo interactivo. [29] **Ilustración No. 6**

ILUSTRACIÓN 6 CUADRO EXPLICATIVO DE LOS ELEMENTOS DE LA TECNOLOGÍA DE INFORMACIÓN

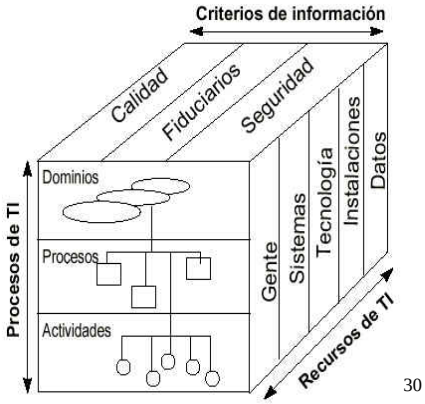


Los recursos de T.I. son administrados por procesos de T.I., los cuales permiten al área de informática la entrega de servicios para que la organización pueda cumplir con sus objetivos. La norma ISO/IEC-20000 impulsa el uso de un enfoque integral de gestión de procesos para brindar servicios que satisfagan las necesidades de los clientes y requerimientos del negocio.

Al hablar de las TI debemos considerar un entorno en donde se interrelacionan los recursos de T.I, para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, el marco conceptual se puede abordar desde tres puntos de vista: los criterios de información, los recursos de TI y los procesos de TI. Estos tres puntos de vista se muestran en el Cubo de COBIT como se muestra a continuación.

[29] The risk IT framework

ILUSTRACIÓN 7 **CUBO DESCRIPTIVO DE COBIT, RECURSOS, PROCESOS Y CRITERIOS DE T.I.**



30

COBIT es un marco de referencia aceptado internacionalmente como una buena práctica de control de la información, desarrollado por la información Systems Audit and Control Association, (ISACA) y el IT Governance Institute (ITGI) con un equipo de más de 100 expertos alrededor del mundo (miembros de ISACA y otras industrias) y es utilizado para implementar el gobierno de TI y mejorar los controles de TI. Se trata de un marco compatible y que incorpora aspectos fundamentales de otros estándares y modelos relacionados (COSO, CMM, ISO 27005 y BS7799). Su misión es investigar, desarrollar publicar y promover un conjunto de objetivos de controles de tecnología de información rectores, actualizados, internacionales y generalmente aceptados por Gerentes de negocio y personal de TI. **(Ilustración No. 7)**

Principios básicos de COBIT

Para satisfacer esta necesidad COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

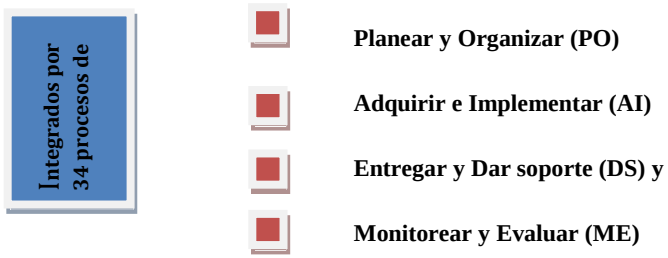
La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente como consejero para la gerencia y para los propietarios de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio, gráfico No.8: proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información. El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

Con respecto a orientado a procesos COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son:

[30] Risk IT

ILUSTRACIÓN 8 DIVISION DE LOS 34 PROCESOS DE COBIT

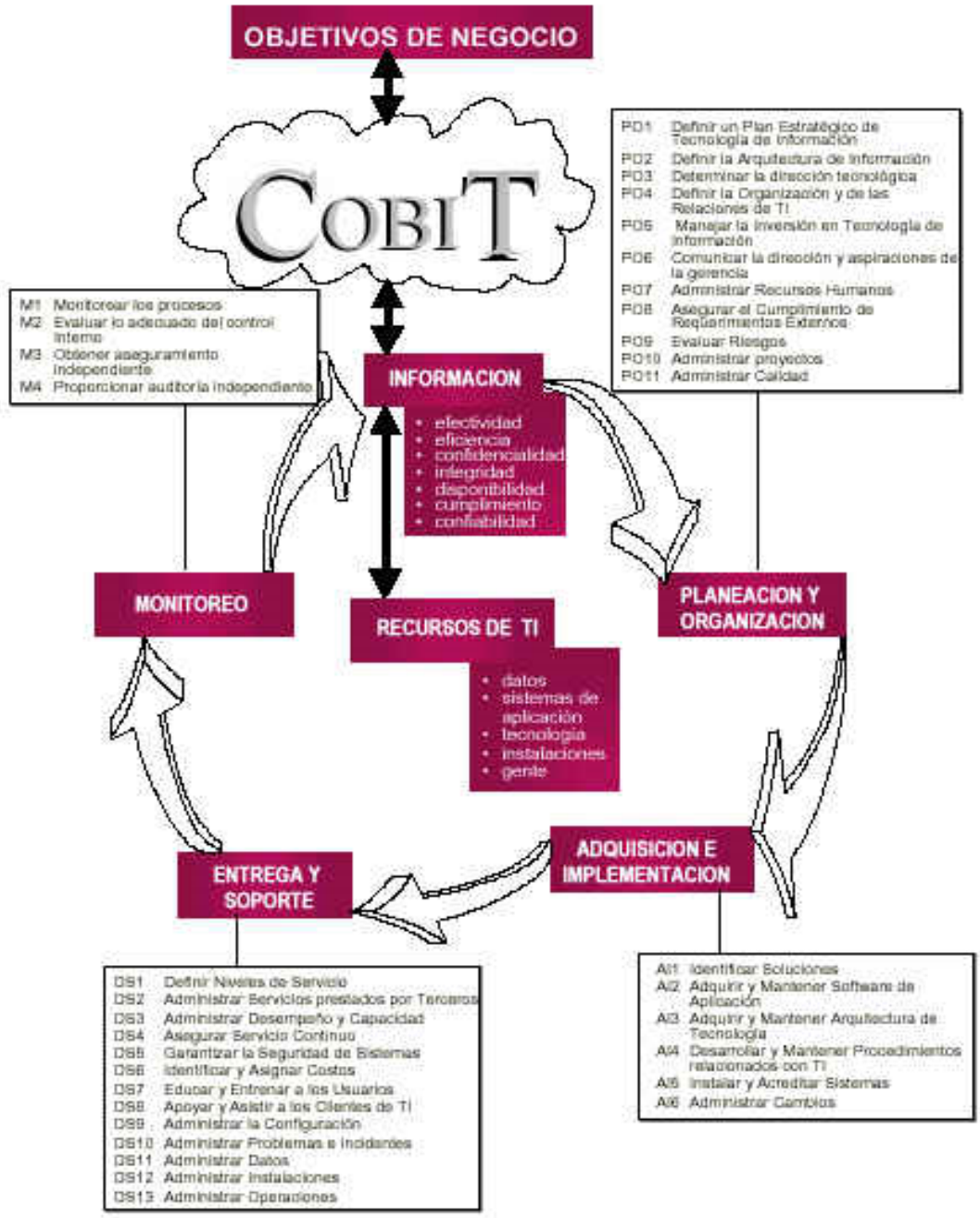


Cada proceso tiene cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso.

Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional 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 administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades. **Ilustración No. 8**

ILUSTRACIÓN 9 **CUBO DESCRIPTIVO DE COBIT, RECURSOS, PROCESOS Y CRITERIOS DE T.I.**

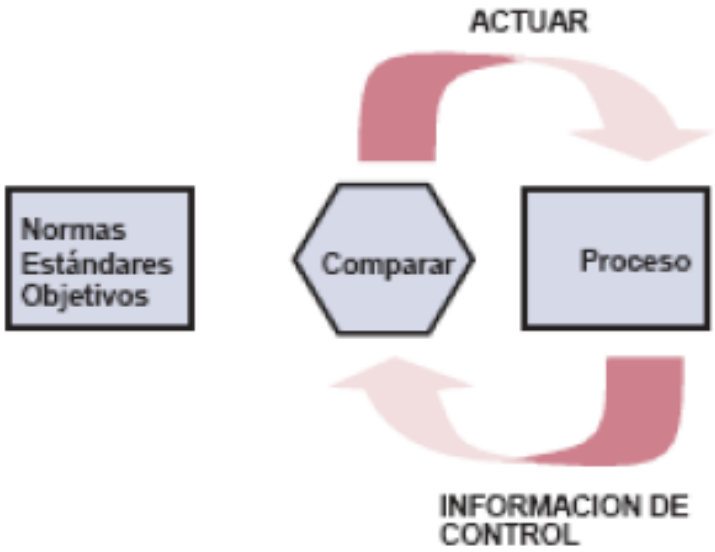


En la parte que está **Basado en controles,** se refiere a que los procesos requieren controles; control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una

actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT.

La guía se puede obtener del modelo de control estándar mostrado en la figura. Sigue los principios que se evidencian en la siguiente analogía: cuando se ajusta la temperatura ambiente (estándar) para el sistema de calefacción (proceso), el sistema verificará de forma constante (comparar) la temperatura ambiente (Inf. De control) e indicará (actuar) al sistema de calefacción para que genere más o menos calor. **Ilustración No.9**

ILUSTRACIÓN 10 **MODELO DE CONTROL DE COBIT.**

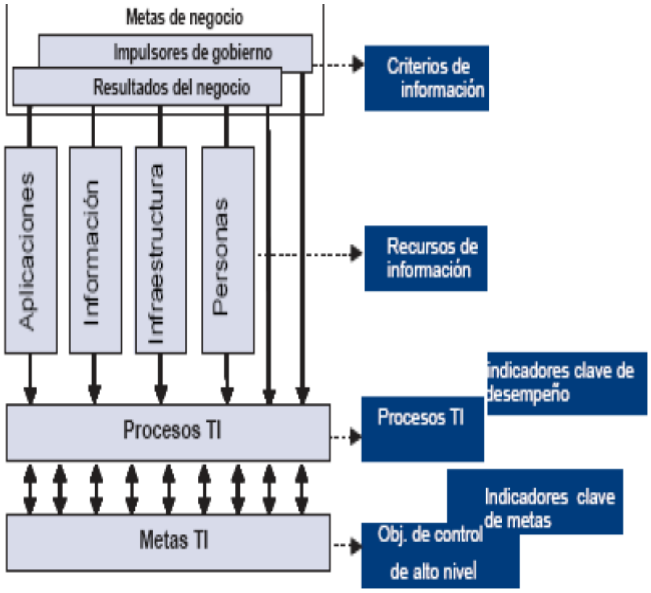


La gerencia operacional usa los procesos para organizar y administrar las actividades de TI en curso, COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia operacional de TI y para la gerencia administrativa. Para lograr un gobierno efectivo, los gerentes operacionales deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y controles de TI. **(Véase Ilustración No.10)**

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa. La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. Para decidir cuál es el nivel correcto, la gerencia debe preguntarse a sí misma: ¿Qué tan lejos debemos ir, y está justificado el costo por beneficio? COBIT atiende estos temas para generar mediciones, por medio:

- ✓ Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.
- ✓ Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos (internos basados en los principios de un marcador de puntuación balanceado (Balanced Scorecard).
- ✓ Metas de actividades para facilitar el desempeño efectivo de los procesos. **(véase Ilustración No.11)**

ILUSTRACIÓN 11 **LOS MODELOS DE INTERACCIÓN DEL NEGOCIO Y RECURSOS DE TI**



➢ Agrupamiento lógico de procesos, a menudo se concibe como dominios de responsabilidad dentro de una estructura y encuadra en el ciclo de vida aplicable a los procesos de TI.
➢ Una serie de actividades o tareas vinculadas con cortes (de control) naturales.
➢ Son necesarias para lograr un resultado mensurable. Son las acciones que deben realizarse para que el proceso cumpla con su objetivo.

Beneficios del COBIT

Algunos de los beneficios que se obtienen al implementar COBIT son los siguientes:

- Mejor alineación, con base en su enfoque de negocios.
- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores.
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común.
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI, (COBIT, 2005).

2.5.2.- LA IMPORTANCIA DE LAS T.I. EN LA ACTUALIDAD

En la actualidad, los negocios bursátiles se vuelven más competitivos por varios aspectos, entre los que destacan: el incremento de su eficiencia productiva, la mejora en la calidad de sus productos y servicios y cualquier respuesta positiva inmediata que se tenga ante las necesidades del cliente.

Para poder lograr estos objetivos, muchos de los negocios bursátiles que han tenido éxito en su estrategia ha sido mediante el uso de las tecnologías de información, las cuales han tenido un impacto positivo en el desempeño de las funciones de estas compañías. Existen formas de medir el impacto que la inversión en TI está teniendo para los negocios en cuestión y si es o no conveniente invertir lo que se está pagando por automatizar sus procesos. Lo anterior hace necesario que tanto el personal de la empresa como los administradores comprendan la sinergia que las TI producen. De esta manera los administradores de empresas impulsaran soluciones con base en las TI.

Hoy por hoy, los negocios buscan soluciones de información que les permitan competir en el mercado global, el reto es encontrar métodos eficientes para que las tecnologías de información reúnan las características que el negocio requiere, es decir, el nivel de asociación de la tecnología con un planteamiento de cambio en el modelo del negocio.

El rol de las tecnologías de información en las organizaciones bursátiles ha cambiado radicalmente de ser un simple soporte de oficina hasta llegar a formar parte de la estrategia competitiva de la compañía y de esta manera incrementar la eficiencia operacional, así como mejorar los productos y

la calidad de los servicios que ofrecen. Al implementar nuevas TI, los negocios tendrán una adopción rápida de tecnología que les permitirá bajos costos y tener un buen control de sus bases de datos de clientes, proveedores y distribuidores.[31]

2.5.3.- LA GESTIÓN DE LAS T.I. EN LAS EMPRESAS PARTICIPANTES EN EL MERCADO DE VALORES

Ante la necesidad de una gestión de la TI dentro de las empresas participantes en el mercado de valores ecuatoriano, deben de basar sus operaciones considerando los principios emitidos por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), institución que ha propuesto los objetivos de control para la Información y la Tecnología relacionada (Cobit) como un modelo de referencia desde un enfoque de control. La misión de Cobit es investigar, desarrollar, publicar y promover un conjunto de objetivos de control para TI, con autoridad, actualizados, de carácter internacional. Cobit es el resultado del análisis de diversos estándares internacionales existentes en el área de control de TI.

La gestión de TI debe estar alineada con la estrategia del negocio, ser su soporte operativo. Así que mencionaremos 2 puntos muy importantes para dicha actividad:

- La gestión de los procesos de TI tiene como función identificar los procesos claves de la empresa para que trabajen de una manera adecuada y funcione como un todo que gestione la información de forma eficaz y eficiente para la empresa. Un ejemplo claro de dicha gestión la hace COBIT en sus 4 dominios. Lo importante es que la gestión de los procesos de TI sea global como un todo en donde todos son procesos claves.
- La gestión de los servicios de TI se refiere a alinear los servicios soportados o entregados por las TI conforme a las necesidades del usuario, esto surge debido a la necesidad de calidad de la gestión de los servicios de TI. Tanto ITIL, COBIT, y ISO/IEC 27000 hacen aportaciones muy importantes a esta gestión.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados.

[31] http://www.gestiopolis.com/Canales4/mkt/simparalas.htm

ILUSTRACIÓN 12 CRITERIOS DE CONTROL DE LA INFORMACIÓN

En base a esta información la tecnología de Información hace a las empresas participantes en el mercado de valores más eficientes en: Finanzas virtuales, Servicios Financieros en línea, oficina electrónica, Rol actual del CFO, Información financiera oportuna, automatización de transacciones financieras y bursátiles.

La competitividad tan fuerte que se vive en la actualidad, en conjunto con la globalización y el enfoque en el aspecto ético, ha provocado la tendencia de cambio en las empresas del mercado de valores en sus sistemas de información para la toma de decisiones. Los sistemas de información han sido afectados continuamente por los desarrollos tecnológicos y con el uso del internet se puede contar con información útil, confiable y relevante en tiempos reales. Las empresas bursátiles que cuentan con una adecuada tecnología de información poseen una estrategia competitiva que les puede garantizar éxito en su sector o industria.

Las empresas participantes en el mercado de valores están creando estructuras, productos y estrategias con el objetivo de controlar las llamadas redes de valor. Estas están siendo creadas cuando las instituciones financieras colaboran para ofrecer a sus clientes paquetes de servicios financieros completos, y la única forma de ofrecerlos de manera competitiva es confiar en las tecnologías de información. La tecnología está permitiendo evolucionar de lo tradicional a lo virtual. **Ilustración No.12**

El presente documento tiene como objetivo describir las etapas del modelo del negocio, requerimientos, análisis y diseño del sistema y la presentación del sistema de Automatización de la

Gestión y Evaluación de la Clasificación de Riesgos a la Seguridad de Información, aplicando conceptos de la metodología NIST y apoyándonos en la norma ISO 27005.

La institución participante en el mercado de valores para objeto de estudio y para ella, se ha previsto la elaboración de un sistema que permita automatizar los procesos para identificación, análisis, evaluación, medición y control de riesgos de la seguridad de información.

En el siguiente cuadro podemos visualizar el planteamiento del sistema propuesto que permitirá agilizar y controlar las actividades de pre y post clasificación de riesgos de seguridad de la información permitiendo a los altos directivos y al analista de riesgos dedicarse plenamente a sus labores y de acuerdo a las metas de negocio. **Ilustración No. 13**

ILUSTRACIÓN 13 **Cuadro de Unión de las metas de negocio con las Metas de TI**

[32]

		Metas de negocio	Metas de TI									Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Perspectiva financiera	1	Expandir el porcentaje de mercado	25	28								X	X					
	2	Aumentar el ingreso	25	28								X	X					
	3	Retorno sobre la inversión	24										X					
	4	Optimizar el uso de recursos	14									X	X					
	5	Administrar los riesgos del negocio	2	14	17	18	19	20	21	22				X	X	X		
Perspectiva del cliente	6	Aumentar la orientación y el servicio al cliente	3	23								X						
	7	Ofrecer productos y servicios competitivos	5	24								X	X					
	8	Disponibilidad del servicio	10	16	22	23						X				X		
	9	Agilidad para responder a los requisitos cambiantes (tiempo para comercializar)	1	5	25							X	X					
	10	Optimización de costos y prestación del servicio	7	8	10	24							X					
Perspectiva interna	11	Automatizar e integrar la cadena de valor empresarial	6	7	8	11						X	X					
	12	Mejorar y mantener la funcionalidad del proceso de negocios	6	7	11							X	X					
	13	Disminuir los costos de los procesos	7	8	13	15	24						X					
	14	Cumplimiento de leyes y reglamentos externos	2	19	20	21	22	6	27					X			X	
	15	Transparencia	2	18														X
	16	Cumplimiento de políticas internas	2	13										X			X	
	17	Mejorar y mantener la productividad operativa y del equipo de trabajo	7	8	11	13						X	X					
Perspectiva de aprendizaje y crecimiento	18	Innovacióon del producto/negocio	5	25	28							X	X					
	19	Obtener información confiable y útil para la toma de decisiones estratégicas	2	4	12	20	26					X			X			X
	20	Adquirir y mantener personal capacitado y motivado	9									X	X					

[32] Cobit 4 Apéndice II y III

2.5.4.- VENTAJAS Y DESVENTAJAS DEL USO DE LAS T.I. EN LAS EMPRESAS

Ya que el fin principal de esta tesis es: proponer una solución que reduzca la situación actual de baja seguridad por la que pasan las tecnologías de información y la relevancia de su contenido; y dado que las TI se encuentran inmersas en todos los aspectos de la empresa, es conveniente comprender los beneficios y daños por los que podría transitar la empresa en el uso adecuado e inadecuado de estas tecnologías; por ello y a continuación se agrega un cuadro comparativo con estos argumentos que permita aclarar y reconocer la importancia del buen tratamiento de la información en las TI y su suceso contrario. **Ilustración 14**

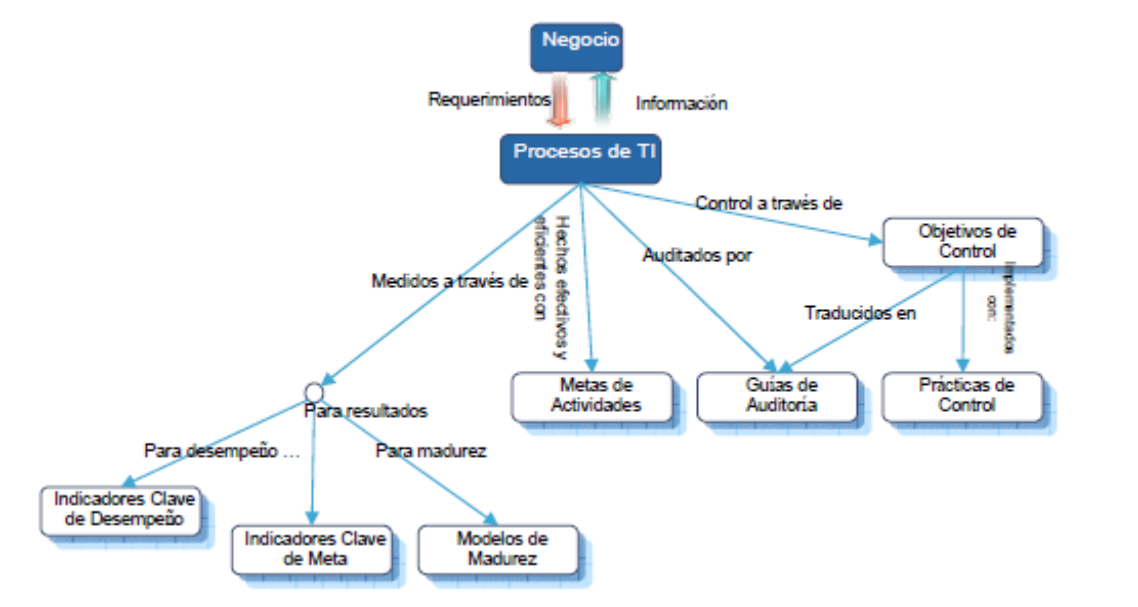
ILUSTRACIÓN 14 CUADRO COMPARATIVO DE LAS VENTAJAS Y DESVENTAJAS DEL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN.

Eficaz y adecuado:	**Ineficaz e incorrecto:**
• Facilita la información exacta oportuna y relevante acerca de la empresa a todos los niveles, desde el personal operativo hasta la dirección administrativa. • Permite el procesamiento sin obstáculos de cada aspecto de los procesos del negocio de ese modo mejora la productividad y eficacia de todo el personal operativo. • Va más allá del proceso transaccional y de la administración de la información para generar ventajas competitivas para la empresa de varias maneras. • Evitar gastos innecesarios en TI.	• Puede causar un daño significativo a los negocios por pérdida de ventaja competitiva. • Ineficiencia que termina en un servicio pobre a los clientes. • Incremento de costos • Aumento en los ciclos de procesos • Tiempos muertos. 33

Ahora que se ha informado de las ventajas y desventajas que se producen del uso de las TI, a continuación se presenta un análisis y diagnóstico de estándares, marcos y modelos que proponen medidas importantes y mejores prácticas al permitir dar un buen uso a las TI y salvaguardar la información contenida en éstas; afinando como resultado, un medio ambiente de seguridad correcto.

[33] http://www.monografias.com/trabajos45/tecnologias-y-planificacion/tecnologias-y-planificacion2.shtml

ILUSTRACIÓN 15 **CONCEPTOS USADOS POR COBIT.**

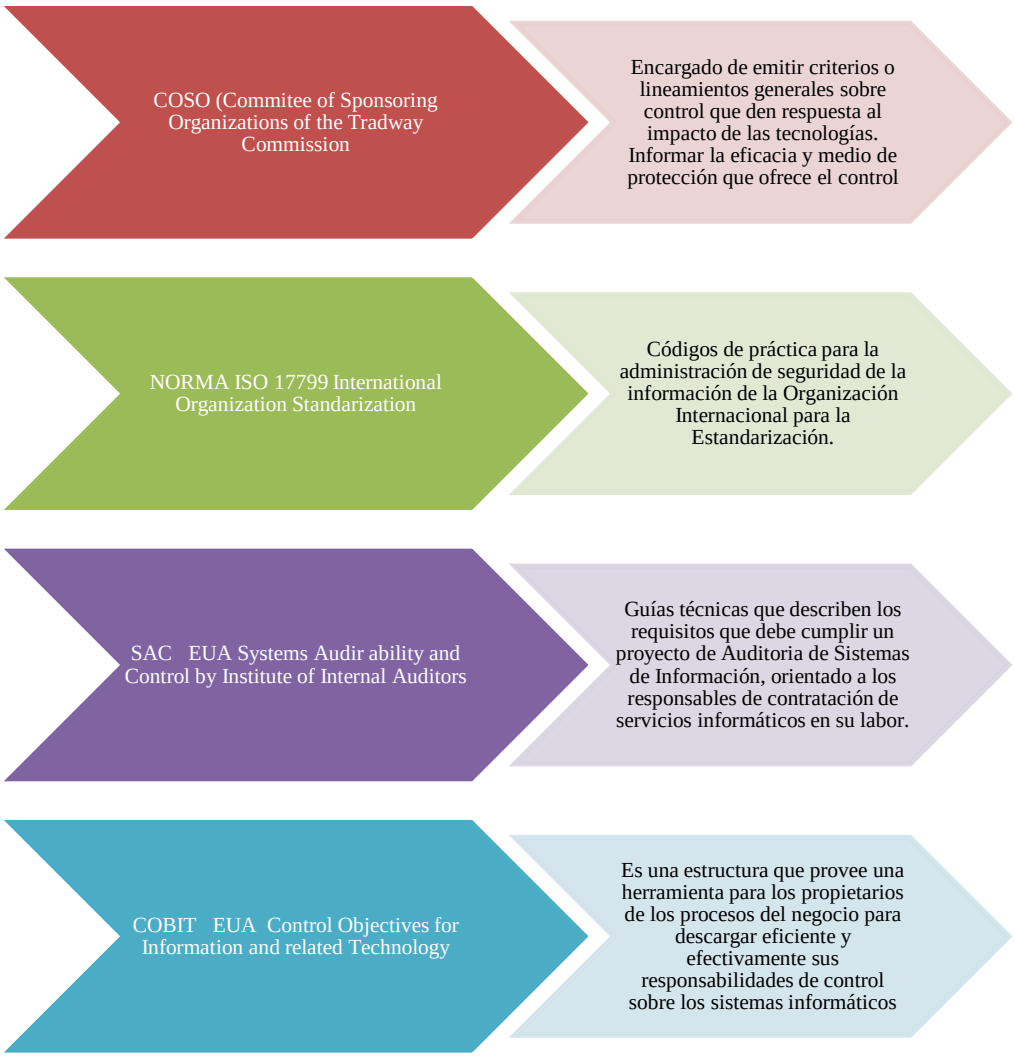


El cuadro explica claramente como los procesos de TI con sus respectivos objetivos de control de seguridad, metas de las actividades, guías de auditoría y prácticas de control afectan a los resultados del negocio por lo cual es elemental los indicadores de clave de desempeño, claves de meta y modelos de madurez. Los principios de COBIT a este respecto se explican de manera más ejemplificada en la **Ilustración No. 15**

2.6.- ANÁLISIS, EVALUACIÓN Y DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LOS MARCOS EXISTENTES DE ADMINISTRACIÓN DE RIESGOS CON RELACIÓN A LAS T.I.

En el siguiente esquema, se muestran modelos, marcos y estándares utilizados para el control interno aplicados a las TI, los más utilizados a nivel de Latinoamérica.

ILUSTRACIÓN 16 MARCOS EXISTENTES RELACIONADOS A LA ADMINISTRACIÓN DE RIESGOS DE T.I.



Definidos los estándares o marcos que contienen las mejores prácticas más comúnmente utilizados en Latinoamérica; ahora, como un breve síntesis se presenta el siguiente cuadro comparativo que muestra el modelo COSO (usado para el control interno en general) y el marco COBIT (utilizado para el control interno en las TI); se ha adicionado a éste cuadro, el conjunto de medidas para las tecnologías SAC como referencia; debido a que el marco COBIT surge de la suma del COSO y el SAC, lo que permite considerarlo como un marco referencial más completo e integral. **Ilustración No. 16**

ILUSTRACIÓN 17 **ANÁLISIS COMPARATIVO DE LOS MARCOS DE CONTROL INTERNO Y CONTROL APLICADO A LAS TI CON RELEVANCIA EN LATINOAMÉRICA**

ANÁLISIS COMPARATIVO DE LOS MARCOS DE CONTROL INTERNO Y CONTROL APLICADO A LAS TI CON RELEVANCIA EN LATINOAMÉRICA			
Marco de Control Interno	Control Interno	Tecnologías de Información	Control Interno aplicado a las Tecnologías de Información
	COSO (Committee of Sponsoring Organizations of the Tread way Commission)	SAC(Systems Audit ability and Control)	COBIT (Control Objectives for Information and related Technology)
Descripción:	Coso. Internal Control-Integrated framework del Committee of Sponsoring Organizations of the Tread way. Commission. Publicado en EUA en 1992 en respuesta a las inquietudes que planteaba la diversidad de conceptos y definiciones e interpretaciones existentes en torno al control interno	SAC, Fundation SAC (1991, revisado en 1994) ofrece asistencia a los auditores internos sobre el control y auditoría de los sistemas y tecnología informática.	Cobit (Control Objetives for Information and related Technology)of Information Systems Audit and Control Fundation COBIT (1996) es una estructura que provee una herramienta para los propietarios de los procesos del negocio para descargar eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos
Dirigido a:	Auditores Internos	Dirección, usuarios, auditores de Sistemas de Información	Auditores Internos
Se refiere al control Interno como:	Procesos	Conjunto de procesos, subsistemas y personas	Conjunto de procesos incluyendo políticas, procedimientos, prácticas estructuras organizacionales.

Por consecuencia, se puede dar el siguiente diagnóstico:

Algunas de estas actividades que se podrán realizar y que no se proponen o contemplan en el modelo a conseguir son las siguientes:

- Identificar o adquirir el medio ambiente general y particular de TI, así como el conocimiento detallado de sus procesos como apoyo para el diseño de actividades y objetivos de control para TI.
- Detallar el desarrollo de una estructura de controles para llevar un registro y evaluación de éstos.
- Explicar y aplicar de manera adecuada algunas de las técnicas particulares de apoyo para crear un ambiente de seguridad. **Ilustración No.17**

Por lo tanto, existe una necesidad de proponer una Metodología para el establecimiento de objetivos de control y sus actividades correspondientes, para lograr un menor índice de exposición a los riesgos en tecnología de información.

CAPÍTULO III.- INTRODUCCIÓN AL RIESGO DE TECNOLOGÍA DE INFORMACIÓN DENTRO DE LAS EMPRESAS PARTICIPANTES EN EL MERCADO DE VALORES

3.1.- ¿QUÉ ES UN RIESGO?

Existen varias acepciones de lo que es el riesgo, como por ejemplo:

- "Procede del latín riscare, significa atreverse, estar en un lugar peligroso. Es el peligro inherente que acompaña a una determinada actividad"[34].
- "Contingencia o proximidad de un daño….."[35]
- "Peligro, contratiempo posible (…) Daño, siniestro eventual garantizado por las compañías de seguros el pago de una prima (…). A riesgo de, exponiéndose a"[36].
- "La posibilidad de perder una inversión determinada. El riesgo suele asociarse a la incertidumbre. El riesgo no necesariamente es malo, ya que en la medida que incrementa se logra un premio. Así por ejemplo, los títulos de crédito que conllevan mayor riesgo. En los instrumentos de renta fija, en que el riesgo es menor, no suele haber la posibilidad de ganancias de capital sustanciosas que en renta variable con riesgo, sí hay ganancias de capital sustanciosas (o pérdida-de ahí el riesgo). El riesgo es un factor distintivo entre el empresario y rentista. El empresario acepta el riesgo y limita sus ganancias; el rentista prefiere ganar menos, en forma estable, pero no arriesgar".[37]
- "La posibilidad de varianza de los resultados esperados (...) es elemento sorpresa de rendimiento real, donde el otro elemento es el resultado esperado".[38]
- "Riesgo financiero se entiende como la diferencia entre el rendimiento actual y el rendimiento esperado. Probabilidad de ocurrencia.

De igual forma, riesgo financiero es el riesgo de posible insolvencia y la variación en las utilidades disponibles para los poseedores de acciones ordinarias.[39]

En finanzas, el concepto de riesgo está relacionado con la posibilidad de que ocurra un evento que se traduzca en pérdidas para los participantes en los mercados financieros, como pueden ser inversionistas, deudores o entidades financieras. El riesgo es producto de la incertidumbre que existe sobre el valor de los activos financieros, ante movimientos adversos de los factores que determinan su precio; a mayor incertidumbre mayor riesgo.

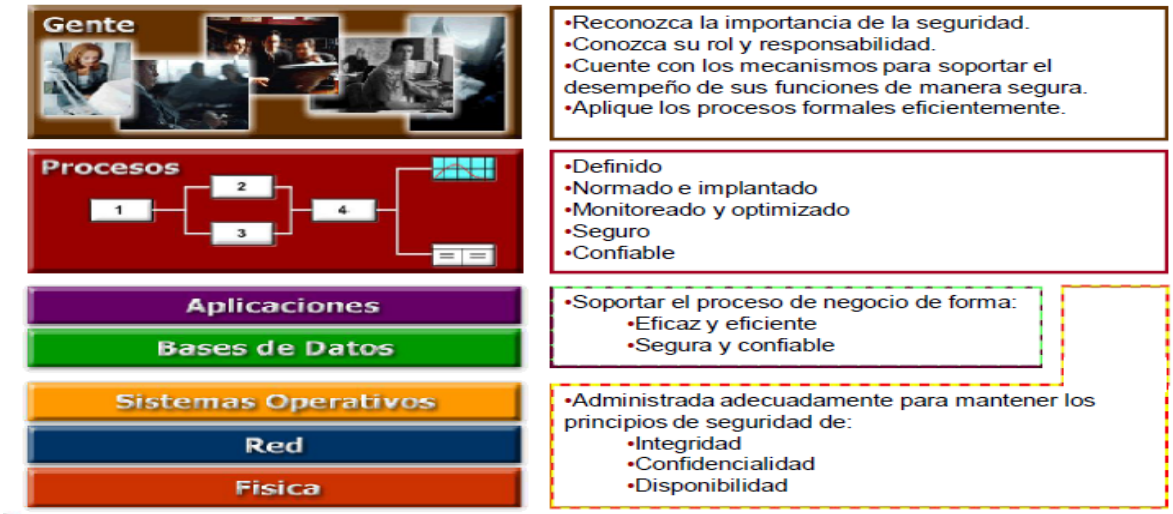
Por otro lado de acuerdo con (COVENIN 2270:1995) el riesgo es "una medida potencial de pérdida económica o lesión en términos de la probabilidad de ocurrencia de un evento no deseado junto con la magnitud de las consecuencias. Así mismo el riesgo es la amenaza concreta de daño que yace sobre la gente en cada momento y segundos de sus vidas, pero que puede materializarse en algún momento o no.

[34] MexDer, Publicaciones especiales
[35] Enciclopedia Rial pH
[36] Diccionario de la Real Academia de la Lengua Española
[37] Cortina Ortega Gonzalo, óp. cit,p. 157
[38] Van Horne,op cit p. 179
[39] Morales Castro Arturo, op cit, p. 68

Para efectos de esta investigación entenderemos por riesgo a la probabilidad de que suceda un evento, impacto o consecuencias negativos. Así mismo lo entenderemos también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento.

Para un mayor entendimiento el siguiente cuadro muestra que debe de contemplar el análisis de riesgos. **Ilustración No. 18**

ILUSTRACIÓN 18 CUADRO EXPLICATIVO DE LO QUE ABARCA UN ANÁLISIS DE RIESGOS



Por otro lado riesgo en informática, según la norma ISO 27005-2008, un "riesgo" se entiende como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Así que para los fines de esta tesis, podemos concluir que un riesgo de TI es cualquier suceso que ponga en peligro los procesos críticos que son soportados por las TI y afecten de manera significativa a la empresa.

Esta Norma proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una Organización.

Sin embargo, esta Norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

3.2. FACTORES DE RIESGO EN T.I.

La T.I. es un elemento estratégico cuyos riesgos se deben de medir y gestionar rigurosamente debido a los siguientes factores:

1.- Creciente dependencia que tienen las organizaciones de la información y de los aplicativos que la proporcionan.

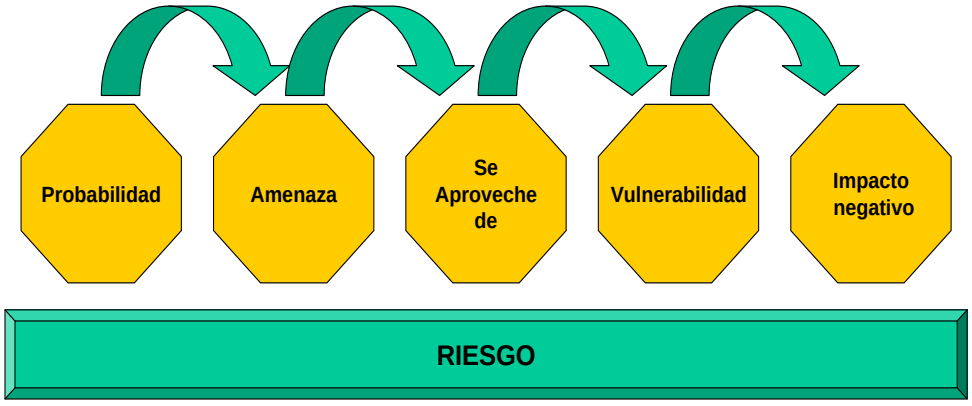
2.- Vulnerabilidad de las redes interconectadas, escala de costos considerable de inversiones en infraestructura y, el valor que la TI debe aportar al negocio, sus productos y servicios.

Por otra parte, siendo la información el activo intangible más importante de una empresa, el responsable de TI debe velar porque las políticas, procedimientos y estructura organizacional, provean una razonable seguridad de que la información se encuentra a salvo de eventos indeseados y que éstos sean prevenidos, detectados o corregidos de manera oportuna, eficaz y eficientemente.

Por lo que se sintetiza en 4 factores claves:

- **Activo**.- Es algo que tiene valor para la organización y por lo tanto requiere protección. Activos / recursos incluyen:
    - La gente y la organización
    - Los procesos de TI, por ejemplo, el modelo como COBIT o Val IT de los procesos de TI, o de los procesos de negocio
    - La infraestructura física, por ejemplo, instalaciones, equipos
    - La infraestructura de TI, incluyendo el hardware de computación, infraestructura de red, middleware
    - Los demás componentes de la arquitectura de la organización, incluyendo:
        - Información
        - Aplicaciones
- **Vulnerabilidad.**- Debilidad inherente al activo. Su presencia no causa daño por sí misma, ya que necesita presentarse una amenaza que la explote. La falta de un control también puede considerarse una vulnerabilidad.
- **Amenaza**.- Una circunstancia o evento que tiene el potencial de causar daño a un activo y por lo tanto a la organización.
- **Impacto.**- Daño causado por una amenaza que explota una vulnerabilidad en un activo y que afecta adversamente el logro de los objetivos de negocio.[40]**Ilustración No. 19**

ILUSTRACIÓN 19 **FACTORES DE RIESGO**



[40] Buenas tareas, disponible en www.buenastareas.com

De acuerdo a esta gráfica determinamos que un riesgo se mide en términos de:

1.- La posibilidad / probabilidad de que ocurra un evento y, 2.- Sus consecuencias- impactos

De acuerdo al Risk IT framework, los factores de riesgo son aquellos factores que influyen en la frecuencia y / o impacto en el negocio de los escenarios de riesgo, ya que pueden ser de diferente naturaleza, y se pueden clasificar en dos categorías principales:

- Factores ambientales: estos se pueden dividir en factores internos y externos, diferenciándose en el grado de control que una organización tiene sobre ellos:
- Factores internos del medio ambiente están, en gran medida, bajo el control de la organización, aunque no siempre sea fácil de cambiar.
- Factores externos del medio ambiente están, en gran medida, fuera del control de la organización.

3.3.- ESCENARIOS DE LOS RIESGOS DE T.I.

Uno de los desafíos para la gestión de riesgos de TI debe identificar los riesgos importantes y relevantes entre todo lo que posiblemente puede relacionarse con TI, considerando la presencia y dependencia de TI en el negocio. Una de las técnicas para vencer este desafío es el desarrollo y el empleo de argumentos de riesgo, Es un enfoque básico para lograr el realismo, visión, compromiso organizacional, mejorar el análisis y la estructura de la compleja cuestión de los riesgos de TI.

Una vez que se desarrollan estos escenarios, que se utilizan durante el análisis de riesgo, donde la frecuencia de la situación realmente está sucediendo y los impactos comerciales son estimaciones.
Ilustración No. 20, muestra que los escenarios de riesgo se pueden derivar a través de dos mecanismos diferentes:

1.- Un enfoque de arriba abajo, en el que se parte de los objetivos generales y se realiza un análisis de los escenarios de riesgos de TI más relevantes y probables que impacten los objetivos de negocio. Si los criterios de impacto están bien alineados con los controladores de valor real de la organización, los escenarios de riesgo relevantes se desarrollarán.

2.- Un enfoque de abajo arriba, en el que se utiliza una lista de escenarios genérico para definir un conjunto de escenarios más concretos y personalizados, aplicados a la situación de la organización individual

Los enfoques son complementarios y deben ser utilizados simultáneamente. De hecho, los escenarios de riesgo deben ser pertinentes y deben estar vinculados con el riesgo real de negocio.

Por otra parte, utilizar un conjunto de escenarios de riesgo genérico ayuda a asegurar que no se pasan por alto los riesgos y proporciona una visión más amplia y completa sobre los riesgos de TI.

Una vez que el conjunto de escenarios de riesgo se define, puede ser utilizado para el análisis de riesgos, donde se evalúa la frecuencia y el impacto del escenario. Un componente importante de esta evaluación son los factores de riesgo, como se muestra en la **Ilustración No. 20**[41].

[41] Risk IT Framework, pag.25

ILUSTRACIÓN 20 RELACIÓN DE LOS ESCENARIOS Y FACTORES DE RIESGO DE T.I.

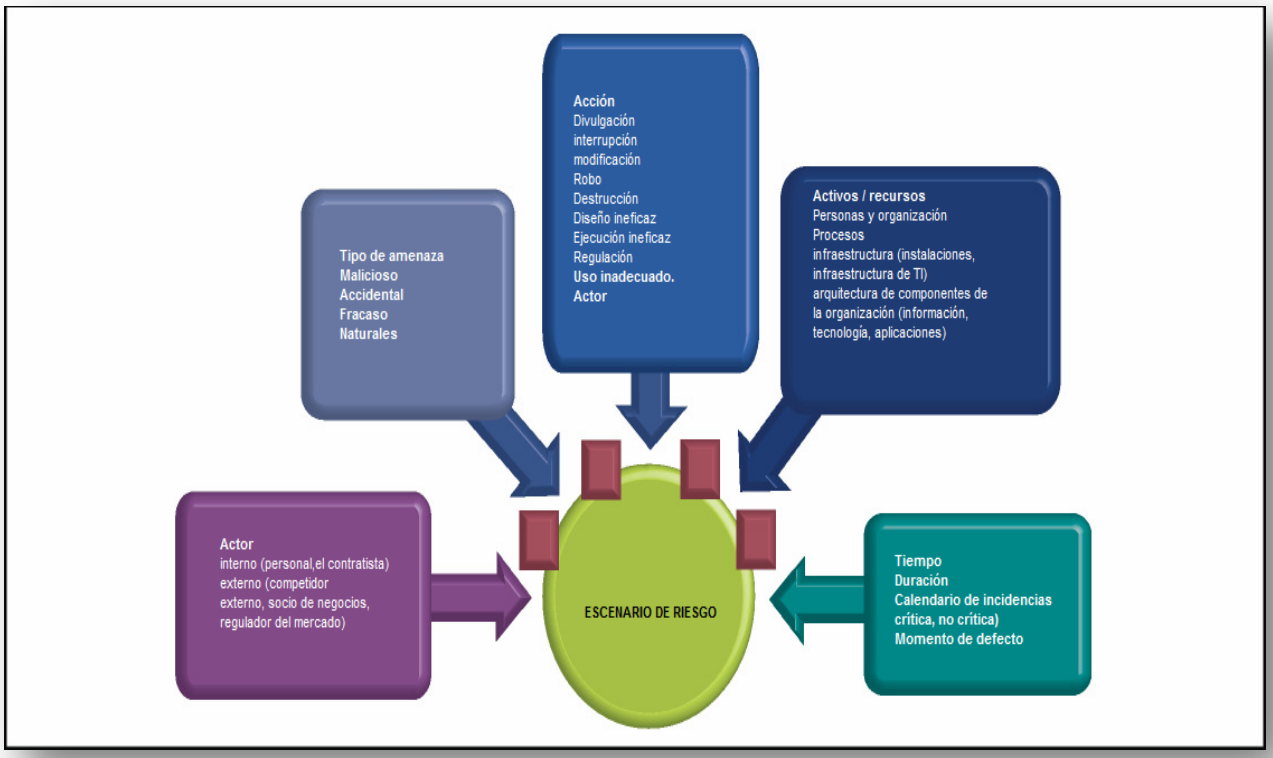
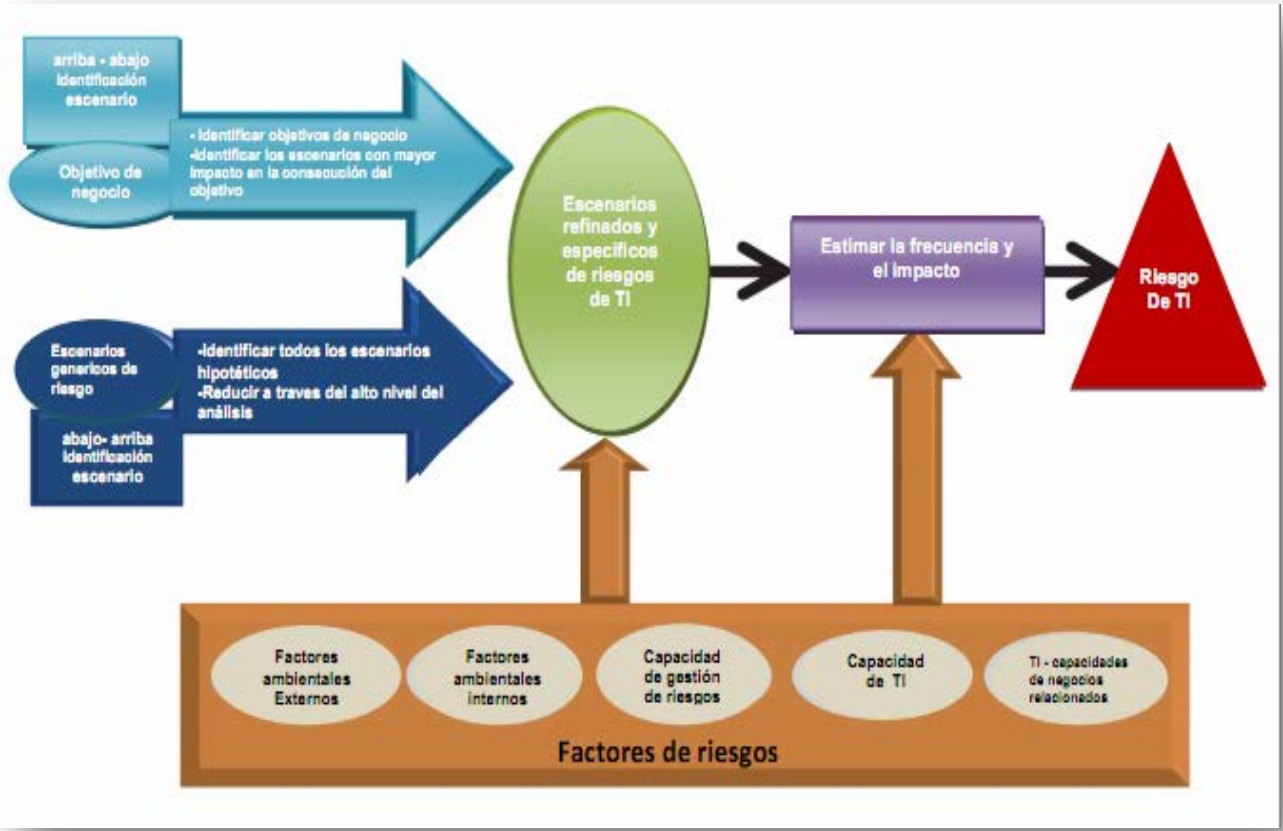


ILUSTRACIÓN 21 **DETALLE DE LOS COMPONENTES DE ESCENARIOS DE RIESGOS DE T.I. SEGÚN RISK I.T.**



3.3.1.- COMPONENTES DE ESCENARIOS DE RIESGOS DE T.I.

El gráfico de escenario de riesgo es la descripción de un evento relacionado con TI que puede conducir a un impacto en el negocio. Para que los escenarios de riesgo sean completos y se puedan utilizar en análisis de riesgos, deben contener los siguientes componentes, que se muestran en la **Ilustración No. 21**

Actor que genera la amenaza - Los actores pueden ser internos o externos y puede ser humano o no humano:

– Los actores internos están dentro de la organización, por ejemplo, personal, contratistas.
– Los agentes externos son extraños, competidores, reguladores y el mercado.

La estructura del escenario de riesgo se diferencia por los eventos de pérdida (la generación de eventos de los efectos negativos), la vulnerabilidad de los eventos (acontecimientos que contribuyen a la magnitud o frecuencia de eventos de pérdida que ocurren), y eventos de amenaza (circunstancias o eventos que pueden desencadenar eventos de pérdida). Es importante no confundir estos riesgos o incluirlos en una lista de grandes riesgos.

3.4.- CLASES DE RIESGOS MÁS COMUNES DEL MERCADO DE VALORES ECUATORIANO

Junto con la posibilidad de flexibilizar, transformar y eliminar los riesgos de mercado, viene también la obligación de hacerlo. Para administrar el riesgo existe la responsabilidad de identificarlo, calcularlo y analizarlo.

En general, hay dos tipos de riesgos:

- Riesgos Intrínsecos: Son propios de la actividad de una compañía, no susceptibles de cobertura. Aquí la capacidad que tienen las empresas para administrar sus riesgos determina su solvencia o riesgo crediticio.
- Riesgos Exógenos: son aquellos que están fuera de control de la compañía, como los riesgos de variaciones indeseables en el tipo de cambio (riesgo cambiario), la tasa de interés (riesgo de tasa de interés) y en algunos casos, en los precios.

Es importante señalar brevemente que en el ámbito bursátil los esquemas de administración de riesgos específicos, los tipos de riesgo más considerables se encuentran:

- Riesgo de mercado.- Es la pérdida potencial ocasionada por movimientos adversos en los precios o tasas de los activos subyacentes. Las medidas preventivas y correctivas al respecto, se relacionan con:

  1.- Monitoreo permanente de los activos subyacentes y los precios de los contratos.
  2.- Valuación diaria de posiciones y colaterales
  3.- Vigilancia de posiciones y ejercicios
  4.- Simulación de situaciones extremas
  5.- Difusión de parámetros de valuación y riesgos
  6.- Liquidación diaria de pérdidas y ganancias

- Riesgo contraparte.- es la exposición a pérdida como resultado del incumplimiento o de la pérdida de la capacidad crediticia de la contraparte. Las medidas preventivas se relacionan con:

  1.- Se efectúa auditoría pre-operativo a los miembros y auditoría diaria a patrimonio Mínimo de los socios liquidadores
  2.- Las garantías se establecen de acuerdo con el riesgo contraparte
  3.- El riesgo contraparte se mutualiza
  4.- El patrimonio mínimo de los socios liquidadores se establece considerando el Máximo nivel del riesgo de cada participante antes de operar.
  5.- Se analiza la capacidad crediticia de cada participante antes de operar
  6.- Se liquida por pago contra entrega, al vencimiento
  7.- Se suspenden las operaciones bajo condiciones de alta volatilidad

- Riesgo Liquidez.- se refiere al costo asociado con falta de liquidez discontinuidad en la formación de precios, amplio spread de compraventa, retraso en la recepción de fondos; las medidas se relacionan con:
  1.- Inversión líquida de corto plazo
  2.- Fideicomisos para ejecución de garantías
  3.- Formadores de mercado

4.- Vigilancia diaria de variaciones de garantías
5.- Suspensiones, cierres o sanciones
6.- Vigilancia diaria de variaciones de garantías
7.- Adecuado manejo de inversión de aportaciones y patrimonio

- Riesgo Humano.- este es generado por falta de capacitación del personal, sobrecarga de trabajo y fallas organizativas. Dentro de las medidas se encuentra:

1. - Estándares de capacitación y Certificación
2.- Separación de áreas de operaciones y administración de riesgos
3.- Auditoría interna y contraloría
4.- Imposición de sanciones por el Comité disciplinario
5.- Actualización de habilidades del personal certificado
6. - Supervision

- Riesgo operativo.- está asociado con errores de ejecución, asignación, administración y control de negociaciones. Las medidas a aplicar son:

1.- Selección operativa de los miembros
2.- Figura de controlar normativo
3.- Establecimiento de manuales operativos y políticas de control de riesgos
4.- Control operativo y vigilancia de riesgo
5.- Descertificación de profesionales
6.- Vigilancia de cumplimiento de parámetros operativos
7- Suspensiones, sanciones y reducción de posiciones

- Riesgo regulatorio.- se refiere a la falta de adecuación del marco normativo
  Medidas preventivas:

1.- Reglas y marco prudencial
2.- Reglamentos y manuales
3.- Estándares de ética y capacitación
4.- Facultades autor regulatorias
5.- Control de riesgos avalado por consejos de administración
6.- Órganos colegiados de autorregulación
7.- Contralor normativo
8.- Revisión permanente del marco normativo
9.- Vigilancia de procedimientos, reglamentos, manuales y políticas

- Riesgo sistémico.- originado como consecuencia de insuficiencias estructurales del sistema financiero y la incapacidad para soportar grandes magnitudes de riesgo de mercado, crédito y liquidación. Las medidas preventivas y correctivas se relacionan con:

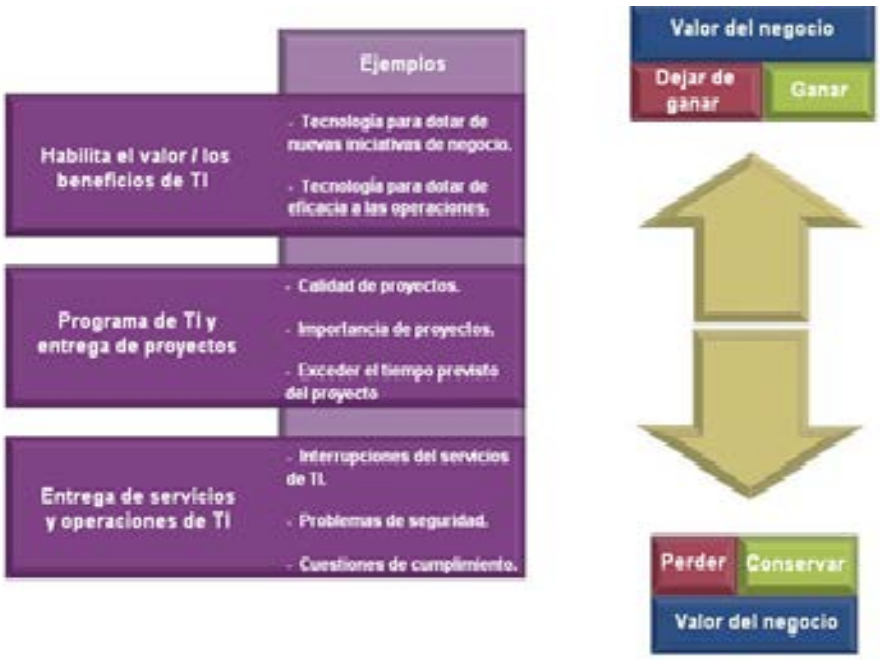
1.- Capital y patrimonio mínimo según riesgo
2.- Posición límite
3.- Socios liquidadores constituidos como fideicomisos
4.- Acciones emergentes de autoridades financieras
5.- Cierre de posiciones
6.- Suspensión de operaciones[42]

[42] Magerit (http://publicaciones,administracion.es) MAGE06] Metodología .de Análisis y Gestión de Riesgos de los Sistemas de Información versión 2, F.López M.A: Amutio J. Candau y J.A. Mañas. Ministerio de Administración Pública, 2006.

3.4.1. CATEGORÍAS DE LOS RIESGOS DE T.I.

Para una mejor comprensión el gráfico que nos plantea Risk IT es claro y específico.

ILUSTRACIÓN 22 **CATEGORÍA DE LOS RIESGOS DE T.I.**



Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio.
Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos. Los riesgos de TI pueden clasificarse de diversas maneras **(véase la Ilustración No.22)**

El público objetivo incluye:

- Los principales ejecutivos y miembros del consejo que necesitan para establecer la dirección y seguimiento del riesgo a nivel de organización.
- Encargados de TI y de los departamentos de negocio que necesitan definir el proceso de la gestión de riesgos.

- Profesionales de la gestión de riesgos que necesitan la dirección específica en cuanto a los riesgos de TI.
- Las partes interesadas externas.[43]

3.5.- ¿QUÉ INCLUYE EL ESTUDIO DE LOS RIESGOS?

La disciplina de gestión de riesgos no es precisamente nueva, pero las amenazas que afrontan las empresas dentro del mercado de valores cambian constantemente y son cada vez más complejas. Los expertos adaptan metodologías de gestión de riesgos para satisfacer las necesidades específicas y proteger la continuidad de sus activos de negocio. La presente tesis busca ayudar a descubrir dónde es más vulnerable la empresa objeto de estudio, identificar el posible impacto y evaluar medidas de seguridad.

El estudio de riesgos y vulnerabilidades incluye la inspección de los siguientes elementos:

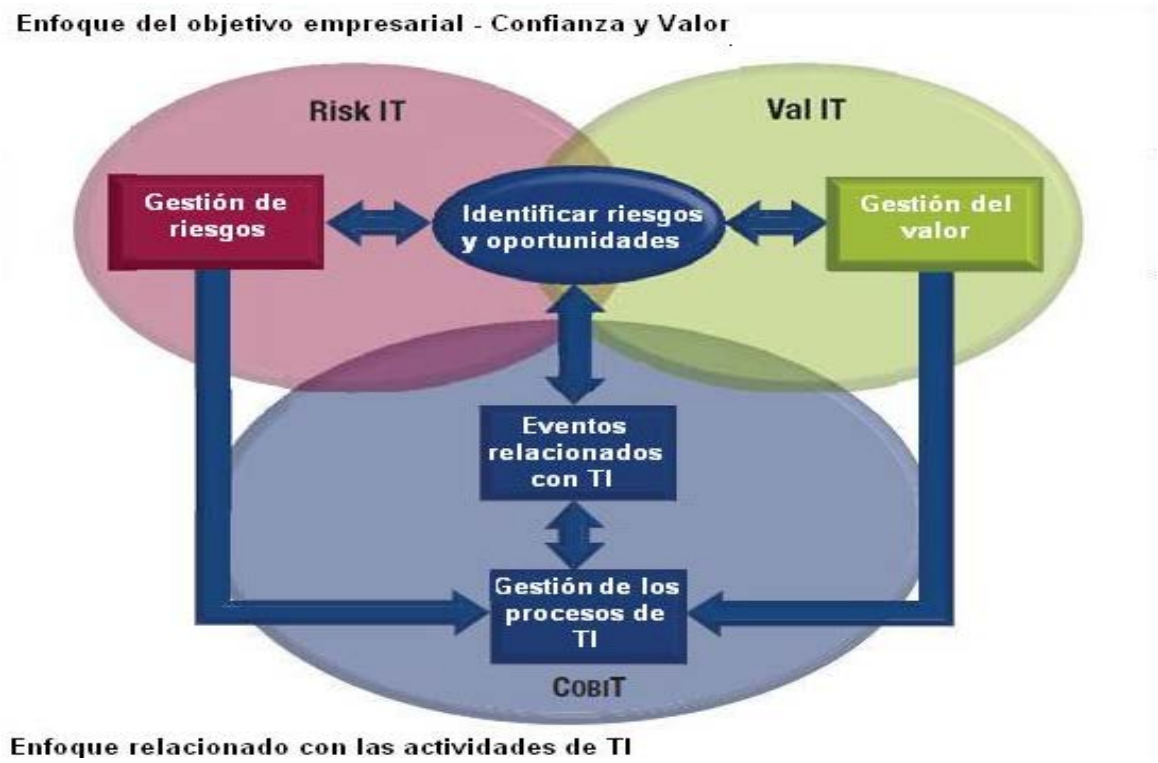
- Físicos: inspección de los elementos eléctricos, mecánicos y estructurales de la instalación
- Lógicos: inspección de las disciplinas de negocio y de TI empleadas para administrar la empresa
- Seguridad: inspección de la seguridad lógica de sus datos e información, así como de la seguridad física del emplazamiento
- Seguridad laboral: inspección de aspectos relacionados con la protección del personal, como la manipulación de paquetes en la sala de correos, políticas y procedimientos de despido y contratación.

Incluye una inspección que relaciona los activos de la organización con aquellas amenazas que pudieran afectar negativamente a la continuidad de negocio y la disponibilidad de información.

[43] Risk IT Framework

3.5.1.- ENFOQUE GENERAL DE UN ESTUDIO DE RIESGOS DESDE LOS MARCOS DE REFERENCIA RISK IT, VAL IT Y COBIT

ILUSTRACIÓN 23 **ENFOQUES RELACIONADOS CON LAS ACTIVIDADES Y RIESGOS DE T.I.**



El marco de los riesgos de TI, RISK IT, se complementa con COBIT, que proporciona un marco integral para el control y la gestión de servicios de TI. Aunque COBIT establece las mejores prácticas para la gestión de riesgos proporcionando un conjunto de controles para mitigar los riesgos de TI, RISK IT establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio.

Estos procesos tienen que tratar con eventos internos o externos a la organización.
Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las fusiones.

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

Estos eventos, plantean un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas. La dimensión del riesgo, y cómo gestionarlo, es el tema principal de RISK IT.[44]

Cuándo se identifican las oportunidades de cambios del negocio relacionados con TI, el Marco VAL IT describe cómo progresar y maximizar el retorno de la inversión realizada en los mismos.

El resultado de la evaluación tendrá probablemente un impacto en algunos de los procesos de TI, por lo que las flechas de la “Gestión de Riesgos" y “Gestión del Valor” se dirigen a la "Gestión de los Procesos de TI", tal y como se muestra en la **(Ilustración No.23)**

3.5.2.- RELEVANCIA E IMPORTANCIA DE UN ESTUDIO DE RIESGOS

En la actualidad los temas relativos a la auditoría informática cobran cada vez más relevancia, debido a que la información se ha convertido en el activo más importante de las empresas, representando su principal ventaja estratégica, por lo que estas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información, con el fin de obtener la mayor productividad y calidad posibles.

Las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adaptarse rápidamente a las nuevas circunstancias para sobrevivir.
Este cambio es muy rápido, está afectando al mundo entero, y su comprensión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los sistemas y tecnologías de información.
Aunque los avances tecnológicos de los últimos veinte años han sido constantes y espectaculares, en los últimos cinco se ha producido una verdadera revolución tecnológica de gran envergadura e impacto para la propia industria informática, así como de consecuencias importantes para el resto de sectores.

Cada vez, con mayor frecuencia, un mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes. Entonces, de igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información, son indispensables. La gerencia, por ende, debe establecer un sistema de control interno adecuado y tal sistema debe soportar debidamente los procesos del negocio.[45]

3.5.3.- VISIÓN GENERAL DE UN ESTUDIO DE RIESGOS DE T.I.

Sin conocer a ciencia cierta cuáles son los riesgos reales a los que se enfrenta la infraestructura de TI es imposible realizar una política de prevención y recuperación ante desastre mínimamente eficaz.

La gestión de la Continuidad del Servicio debe enumerar y evaluar, dependiendo de su probabilidad de impacto, los diferentes riesgos y los factores que conllevan a los mismos. Para ello es preciso conocer:

[44] RISK IT Framework
[45] Risk IT Framework and Val IT Framework Cardiff Caerdydd. (2004) Risk Management Implementation Guide

- Conocer en profundidad la infraestructura de TI especialmente los servicios críticos y estratégicos.
- Analizar las posibles amenazas y estimar su probabilidad
- Detectar los puntos más vulnerables de la infraestructura TI.

ILUSTRACIÓN 24 **VISIÓN GENERAL DEL ESTUDIO DE RIESGOS DE T.I.**

Con los resultados de este detallado análisis se dispondrá de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio. **Ilustración No.24**

La prevención frente a riesgos genéricos y poco probables puede ser muy costosa y no estar siempre justificado, sin embargo, las medidas preventivas de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente económicas.[46]

3.5.4.- VENTAJAS DE UN ESTUDIO DE RIESGOS

Los aspectos más destacados que se obtiene de un estudio exhaustivo de los riesgos es que permite conocer que riesgos plantean la amenaza más grave para los activos del negocio, siendo para el ámbito bursátil la información, el activo más importante. Segundo, establece las medidas de seguridad rentables para mitigar y prevenir riesgos.

Las amenazas con las que afronta el mercado bursátil cambian constantemente y son cada vez más complejas. Se debe de establecer y adaptar metodologías de gestión de riesgos para poder cubrir las necesidades más específicas de la empresa, proteger la continuidad de los activos y descubrir donde la empresa es más vulnerable e identificar el posible impacto y evaluar las medidas de seguridad.

[46] Osiatis, Disponible en: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/vision_general_gestion_servicios_TI/vision_general_gestion_servicios_TI.php

Si bien es cierto no es posible prevenir todas las interrupciones que se puedan presentar en la marcha del negocio pero si se pueden emplear metodologías contrastadas para aceptar, reducir o transferir los riesgos. Lo principal es emprender actuaciones inmediatas que protejan a la empresa frente a aquellos riesgos que pudieran interrumpir las operaciones.

El estudio de riesgos y vulnerabilidades ayuda a identificar y evaluar riesgos operativos, financieros aún los físicos, el mismo que puede incluir hasta inspecciones de las instalaciones e infraestructura lógica de las TI y del negocio vigentes, conocer a detalle los puntos débiles que conllevan a mayores riesgos de interrupción del negocio, de tal forma que sea posible dar prioridad a las técnicas de mitigación adecuadas y ponerlas en práctica.

El estudio de riesgos y vulnerabilidades ayuda a identificar los activos de negocio más expuestos, establecer valores objetivos, valorar vulnerabilidades y repercusiones potenciales y proponer medidas de seguridad y tácticas de mitigación y con esto las ventajas ó beneficios que obtendrá la empresa son:

1.- Asignación de prioridades y determinación de umbrales de riesgo para sus procesos y recursos de negocio esenciales.

2.- Evaluación de las tácticas de gestión de riesgos y costes asociados con diferentes niveles de protección.

3.- Ampliación de su enfoque desde la mitigación de riesgos hasta la prevención proactiva de fallos.

4.- Demostración de la debida diligencia en la gestión de riesgos.

5.- Preparación frente a auditorias de organismos de control legal y del sector.

6.- Adopción de decisiones cualificadas acerca del mejor modo de proteger su empresa.

En síntesis el estudio de riesgos y vulnerabilidades ayuda a conocer mejor los riesgos relacionados con sus activos físicos y de TI lógicos que puedan interrumpir su actividad o degradar la calidad del servicio, incluyendo la identificación de riesgos externos y amenazas auto inducidas. El estudio permite asignar prioridades y evaluar las tácticas de gestión de riesgos y recursos de negocio esenciales que amplía el enfoque y pasa a ser de una simple mitigación de riesgos a la prevención proactiva de la pérdida de activos de negocio de información.

Existe un gran énfasis en los riesgos que tienen que ver con temas como la privacidad, la seguridad, el terrorismo o malas prácticas ejecutivas. Hoy en día las organizaciones modernas dependen en gran medida de las tecnologías de la información, no sólo desde una perspectiva operacional, sino también para gestionar y aprovechar la información con propósitos competitivos. Por ello, el riesgo relacionado con las TI es una importante consideración a tener en cuenta en el actual entorno empresarial.

El resultado de todo ello es que la gestión del riesgo empresarial está comenzando a ser un área increíblemente compleja, y es fácil verse superado por el número de factores y dependencias involucradas. Se debe de considerar el riesgo como parte de su proceso de planificación global de la empresa.

SEGUNDA PARTE: LA GESTIÓN DE RIESGOS ASOCIADOS A LA T.I. EN EL MERCADO DE VALORES ECUATORIANO Y SU APLICACIÓN

CAPÍTULO IV.- GESTIÓN DE RIESGOS ASOCIADOS A LA T.I.

La gestión de riesgos unificando conceptos y simplificándolo, se puede definir como ¨el proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si esta acción ocurre¨. El análisis de riesgos implica: Determinar **qué** se necesita proteger, **De qué** hay que protegerlo y **Cómo** hacerlo. Por lo cual entendemos que la gestión de riesgos son actividades coordinadas para dirigir y controlar una organización con relación al riesgo[47]. La gestión de riesgos permite a una organización identificar que necesita proteger, cómo debe protegerse y cuánta protección necesita, y así invertir sus esfuerzos y recursos efectivamente. Los marcos de referencia que nos guían en la implementación y mantenimiento de una gestión de riesgos son: ISO 31000, IEC/DIS 31010, ISO EC Guide 73, BS /31100, ISO/ IEC 27005, ITGI-The Risk IT Framework, Basilea II, Octave, NIST SP800-30, CRAMM, MAGERIT, TRA Working Guide, Microsoft-SRMG, BS 7799-3, Airmic, Alarm, Irm-ARMS, UNE 71504, AS/NZS 4360.

Para efectos de esta investigación se tomará como referencia la norma ISO-27005, The Risk IT Framework y Cobit.

En mi síntesis puedo indicar que la gestión de riesgos de T.I., es el proceso mediante el cual se van a establecer los mecanismos que le van a permitir a la empresa a disminuir y controlar los riesgos sobre los equipos, sistemas e información de la organización, es decir, es un mecanismo de prevención de pérdidas.

Y hablando de pérdidas la empresa puede prevenir y detectar con este sistema de gestión: fraudes, pérdida de información, violaciones a leyes y reglamentos, pérdida de clientes, pérdida de imagen institucional, fracaso en los proyectos, oportunidad de negocio, errores de operación, pérdida de activos, sabotaje , para citar las más importantes.

Beneficios de implementar un sistema de gestión de riesgos

- Otorga certidumbre a los proyectos de inversión
- Reducción de riesgo operativo=aumento en la confianza de stakeholders
- Contribuye a maximizar los beneficios de la inversión en tecnología
- Detección oportuna de amenazas

[47] ISO IEC Guide 73:2002

- Contribuye a establecer un orden en la empresa
- Detección de oportunidades de mejora en los procesos y sistemas de la organización
- Cumplir con regulaciones internas y externas
- Incide en la reducción del TCO(Total Cost of Ownership)

4.1.- ANÁLISIS DE LA GESTIÓN DE RIESGOS ASOCIADOS A TI SEGÚN LAS NORMAS, ESTÁNDARES, REGULACIONES Y MARCOS DE REFERENCIA

Especificando este análisis, las regulaciones y normas que regulan y tratan el riesgo son:

Comunicación ¨A¨4609 del BCRA para entidades financieras, siendo este el caso del mercado de valores. Esta regulación establece, los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

ISO/IEC 27001.- Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

La seguridad de la información consiste en procesos y controles diseñados para proteger información de su divulgación no autorizada, transferencia, modificación o destrucción, a los efectos de:

- Asegurar la continuidad del negocio;
- Minimizar posibles daños al negocio;
- Maximizar oportunidades de negocios

4.1.1. LEY SARBANES OXLEY (SOX)

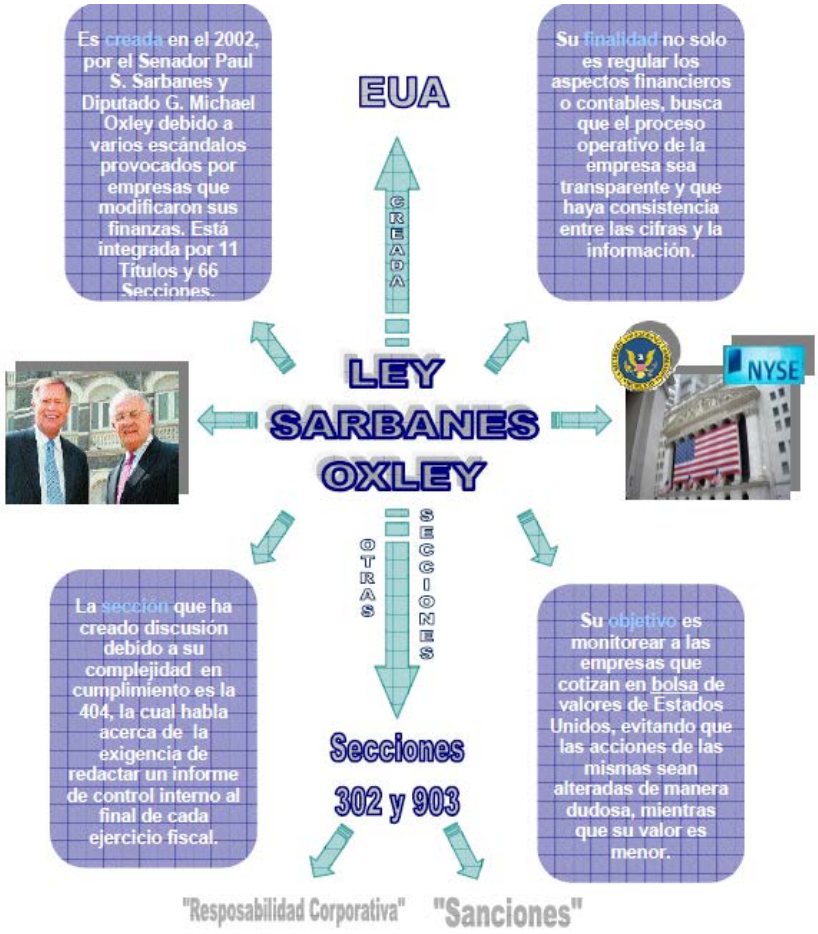
Ley Sarbanes Oxley (SOX), impulsada por el gobierno norteamericano como respuesta a las megas fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros. ISACA ha publicado la segunda edición de la guía IT Control Objetives for Sarbanes-Oxley. Está especialmente orientado a la Gerencia, gestores de TI, así como profesionales de la auditoría en general que tengan que tratar con procesos de validación y conformidad de la Ley Sarbanes-Oxley (SOX). Esta edición contiene la actualización necesaria a raíz de los cambios importantes introducidos por SEC (U.S: Securities and Exchange Commission) y la PCAOB (The Public Company Accounting Oversight Board), al emitir dictámenes que complementan aspectos con implicación, entre otros, en la gestión de riesgo, los controles de aplicación y la evaluación de deficiencias. La Ley Sarbanes Oxley está vigente en EE.UU desde el año 2002 y su propósito es fortalecer los gobiernos Corporativos (de las Sociedades Anónimas) y restituir la confianza de los inversionistas. Esta ley fue promovida por el Senador, Paul Sarbanes y el representante, Michael Oxley.

Se compone por 11 títulos, donde se obliga a cumplir requisitos rígidos para la contabilidad de las empresas. Los diversos títulos y secciones de SOX definen las responsabilidades de administración en los reportes anuales y semestrales, el ambiente de control, **gestión de riesgo,** el monitoreo y la

medición de las actividades de control. Dentro de esta ley, existen 3 secciones que involucran directamente a los departamentos de TI, la 302, 404 y 409:**(véase Ilustración No.25)**

- Sección 302: Responsabilidad Corporativa por los estados financiero: primera fase de SOX entró en rigor desde otoño 2003. Esta sección exige que los gerentes financieros y los gerentes generales certifiquen personalmente y avalen la exactitud de los estados financieros de la empresa.
- Sección 404: Evaluación de la administración del control interno. Es el requerimiento más urgente y demandante de SOX para TI y exige que los auditores certifiquen los controles y procesos de TI requeridos para garantizar los resultados financieros. Esta sección le exige a los auditores, internos y externos, que certifiquen los controles internos y los procesos por los cuales los ejecutivos obtienen la información.
- Sección 409: Liberación en tiempo real de la información requerida. Es el requerimiento más exigente de SOX y está planeado para el futuro. Exige el reporte en tiempo real de eventos materiales que podrían afectar el desempeño financiero de una compañía. El aspecto de tiempo en este requerimiento ejercerá presión significativa sobre la infraestructura actual de TI y las actividades de su administración.[48]

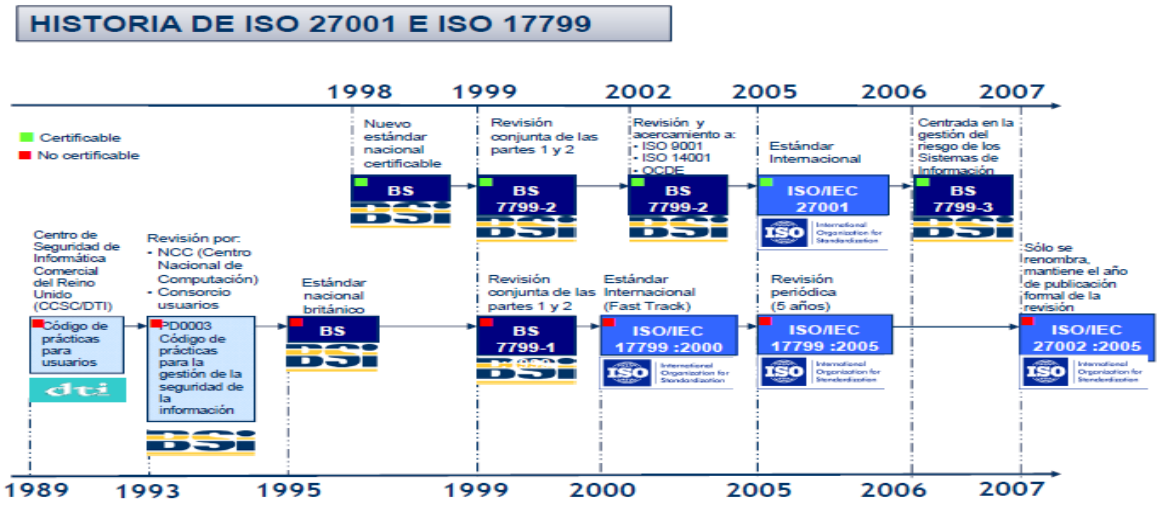
ILUSTRACIÓN 25 **MAPA MENTAL DE LA LEY SARBANES OXLEY**



[48] www.deltasesores.com

4.1.2.- ANÁLISIS BREVE DE LA NORMA ISO-IEC 27005

ILUSTRACIÓN 26 **HISTORIA DE ISO 27001 E ISO 17799**



ISO-IEC 27005.- Esta norma proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una organización. Sin embargo, esta Norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información. Tiene sus inicios desde 1989 **(véase Ilustración No. 26)**

Es aplicable a todo tipo de Organización

- Empresas Comerciales
- Organismos Gubernamentales
- Organismos sin fines de lucro
- Entidades Financieras

La ISO-IEC 27005, se conforma de las siguientes partes:

1.- Establece el contexto
2.- Evalúa el riesgo dentro de este aspecto hay tres puntos:
a.- Identificación del riesgo
b.- Estimación del riesgo
c.- Valoración del riesgo
3.- Tratamiento del riesgo
4.- Aceptación del riesgo
5.- Comunicación del riesgo
6.- Seguimiento del riesgo

La Norma ISO 27005, indica que la seguridad de la información se caracteriza aquí como la preservación de:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información:
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

4.1.3.- ANÁLISIS DE ACUERDO A LA NORMA ISO.31000 (2009)

Según la norma ISO 31000 (2009), la estructura se define a través de los siguientes elementos: compromiso por parte de la dirección, la política de la gestión de riesgos, la cultura de la gestión de riesgos, la alineación con las políticas, objetivos y procesos de la organización, leyes y reglamentos, responsabilidades y recursos.

El compromiso por parte de la dirección, se formaliza con la asignación de responsabilidades, con la autoridad y competencias apropiadas. Las políticas, que son el marco de actuación para la gestión de riesgos, son las guías para que se adopten decisiones, definan objetivos, elaboren planes de tratamientos y asignen recursos. Los reguladores están especialmente preocupados por los riesgos operacionales y sistémicos, no sólo financieros. En el 2001, COSO, inició un proyecto para desarrollar un marco de trabajo para la administración de riesgos (ERM) es marcado por principios, lenguaje común y directrices claras de un correcto manejo de los riesgos.

La política de gestión de riesgos declara:

1.- Promover una cultura de gestión de riesgos
2.- Establecer e implementar una estructura para la gestión de riesgos.
3.- Implementar un conjunto de procesos para la comunicación, identificación, análisis, evaluación y seguimiento de los riesgos.
4.- Proveer información adecuada y oportuna así como formación sobre la gestión de riesgos.[49]

Toda política se instrumenta a través de sus objetivos los cuales son:

- Proteger la calidad de los bienes y servicios entregados;
- Proteger la imagen y la reputación de la organización;
- Proteger los activos de la organización
- Garantizar la integración de los sistemas de información;
- Evitar pérdidas económicas-financieras y fraudes;
- Evitar el incumplimiento de la ley o reglamentos;
- Reducir el costo total de los riesgos.

Para cumplir con las políticas y los objetivos de gestión de riesgos, es necesario que la dirección asigne los recursos necesarios para llevar a cabo los procesos y acciones para disminuir la

[49] COSO, Enterprise Risk marco de gestión de 2004

incertidumbre y mantener bajo control los riesgos. La ISO 31000(2009) lista los siguientes recursos mínimos:

- Las personas con los conocimientos, competencias y experiencias requeridas;
- Los recursos para cada fase de la implantación y mantenimiento de la gestión de riesgos;
- La organización, la estructura, los métodos, los procedimientos y las herramientas necesaria;
- El sistema de información y gestión del conocimiento.[50]

4.2.- PROCESOS ESPECÍFICOS DE APLICACIÓN DE LA GESTIÓN DE RIESGOS DENTRO DE UNA EMPRESA DEL MERCADO DE VALORES ECUATORIANO

Por otro lado, la puesta en marcha de la gestión de riesgos dentro de la organización, se lleva a cabo a través de sus procesos que son: comunicación y consulta, establecimiento del contexto, valoración de los riesgos (identificación, análisis y evaluación), seguimiento y revisión finalmente tratamiento de los riesgos.

Realizando una síntesis breve de estos procesos ya que en el desarrollo de la tesis se ampliará cada proceso, podemos indicar lo siguiente:

Los procesos de operación que se realizan en el mercado de valores del Ecuador son:

1.- Procesos de titularización de cartera.- El responsable es el agente de manejo de valores resultantes de procesos de titularización de cartera, cumplirá con las siguientes funciones dentro de este proceso:

- Determinar el índice de siniestralidad de la cartera a titularizar siguiendo para el efecto las disposiciones de carácter general que determina el Consejo del Mercado de Valores.
- Contar con una declaración juramentada ante autoridad competente del representante legal del originador de que la cartera no se encuentra pignorada ni que sobre ella pesa gravamen alguno
- El monto de emisión no podrá ser superior al saldo insoluto de la cartera al momento de la emisión.

2.- Procesos de titularización de proyectos inmobiliarios.- La titularización de proyectos inmobiliarios consiste en la emisión de títulos mixtos o de participación que incorporen derechos o alícuotas, sobre un patrimonio de propósito exclusivo constituido con un bien inmueble y los diseños, estudios técnicos y de pre factibilidad económica, programación de obra y presupuestos necesarios para desarrollar un proyecto inmobiliario objeto de titularización, el patrimonio de propósito exclusivo también puede constituirse con sumas de dinero destinadas a la adquisición del lote o a la ejecución del proyecto. Dentro de este proceso se debe:

- Emitir solamente valores de participación, o valores mixtos.

[50] ISO 31000:2009 (2009). Gestión del Riesgo, Principios y guías.

- Determinar el índice de desviación en la generación de los flujos proyectados siguiendo el efecto las disposiciones de carácter general que determine el Consejo del Mercado de Valores.
- Contar con dos avalúos actualizados del bien inmueble sobre el cual se desarrollará el proyecto inmobiliario, los cuales deben ser efectuados por peritos independientes del originador y del agente de manejo. Dichos avalúos deben haber sido practicados dentro de los seis meses anteriores a la fecha de iniciación del trámite de autorización de la titularización.
- Obtener una certificación del Registro de la Propiedad, de que sobre los inmuebles objeto de titularización, no pesa ningún gravamen.

- Presentar un estudio técnico económico y de factibilidad del proyecto, la programación y el presupuesto de la obra.

- El constructor debe de construir y mantener a favor del patrimonio autónomo garantías bancarias o pólizas de seguros de fiel cumplimiento del contrato y de buen uso de los anticipos y de los fondos recibidos.
- La obra debe de contar con un fiscalizador de amplia trayectoria para lo cual deberá certificar su experiencia.
- Determinar el punto de equilibrio para iniciar la ejecución del proyecto cuyas características deben constar en el reglamento de gestión. Mientras no se cumpla el punto de equilibrio, los recursos entregados por los inversionistas deben ser entregados a un encargo fiduciario para ser invertidos en papeles de alta liquidez.
- El agente de manejo debe mantener una póliza de seguro contra todo riesgo sobre el inmueble, hasta tres meses posteriores al vencimiento del plazo de los valores producto de la titularización o al prepago de los valores, en los términos establecidos en esta Ley.

  En caso de la titularización de proyectos inmobiliarios, podrá efectuarse por la totalidad o por un segmento de respectivo proyecto, hasta por el monto que fije la disposición de carácter general del Consejo del Mercado de Valores.

3.- Procesos de titularización de activos fijos.- En la titularización de activos fijos se puede emitir valores de participación de contenido crediticio o mixto. Las normas especiales a las que deberán someterse son:

- Determinar el índice de desviación en la generación de los flujos proyectados siguiendo al efecto las disposiciones de carácter general que determine el Consejo del Mercado de Valores.
- Mantener una póliza de seguro contra todo riesgo sobre el activo titularizado, hasta tres meses posteriores al vencimiento del plazo de los valores producto de la titularización, o al prepago de los valores.
- Obtener una certificación del Registro de la Propiedad en el caso de bienes inmuebles, o una declaración juramentada notariada del originador en el caso de bienes muebles, de que sobre los activos fijos objeto de titularización, no pesa ningún gravamen, durante la vigencia del contrato de fideicomiso mercantil;

- Contar con dos avalúos actualizados, los cuales deberán ser efectuados por peritos independientes del originador y del agente de manejo, inscritos en el Registro Nacional de Peritos. Dichos avalúos deben haber sido practicados dentro de los seis meses anteriores a la fecha de iniciación del trámite de autorización de la titularización.

4.- Procesos de titularización de derechos existentes generadores de flujos futuros.- Esta titularización consiste en sustituir activos no líquidos o con bajos niveles de liquidez por liquidez inmediata, mediante la emisión de títulos valores cuya fuente de repago provendrá de los activos transferidos al patrimonio autónomo. En los procesos de titularización desarrollados a partir de derechos existentes generadores de flujos futuros, además del cumplimiento de los requisitos establecidos en las normas especiales contenidas a continuación:

- Presentar estudios económicos y técnicos sobre la generación de los flujos futuros proyectados y el estudio de factibilidad correspondiente, según las características propias de los activos o proyectos.
- Determinar el punto de equilibrio para iniciar el proceso de titularización, cuyas características deberán constar en el reglamento de gestión, de ser el caso.

Con este breve panorama, la gestión de riesgo es una manera de comprender mejor el desempeño de la organización e incluso el de nosotros mismos. Es una herramienta para entender en donde nos movemos y si esto representa un peligro para el logro de lo que nos hemos planteado alcanzar.

Un ejemplo claro son los eventos que actualmente están ocasionado o que ocasionaron pérdidas económicas, deterioran la imagen de la organización, Impactan en los activos, en los bienes y en los servicios entregados. Como la erupción del volcán islandés (2010), el terremoto de Haití(2010) y Chile (2010, control de precios en Venezuela(2007), Inundaciones en Brasil (2010) y Colombia (2010), cierre de la frontera colombo-venezolana (2009), cortes de luz y gas en Argentina(2010), tratados de libre comercio como el Mercosur(1991), política de nacionalización de Venezuela(2007), derrame de petróleo en el golfo de México(2010), Infracciones sobre la propiedad intelectual, seguridad ciudadana, recesión, entre otros.

Sabemos cómo actuar para que estos eventos tengan el mínimo impacto en el logro de los objetivos de la organización, se tiene conocimiento de que estos eventos podrían ocurrir y cuáles serían sus consecuencias.

Anticiparse y estar preparado para actuar y lograr los objetivos de la organización, manteniendo la continuidad de las operaciones es una ventaja competitiva que nos diferencia de nuestros competidores.[51]

4.3.- CLASIFICACIÓN DE LOS RIESGOS ESPECÍFICOS DE T.I. EN UN SISTEMA DE MERCADO DE VALORES

Es importante aclarar que para efectos de esta investigación y al estudio que nos atañe se usa la siguiente clasificación de riesgos, esto con el fin de dar un panorama general de los riesgos de T.I., que afectan a la empresa, por lo que usamos la siguiente clasificación:

[51] Espol, disponible en: www.dspace.espol.edu.ec/

ILUSTRACIÓN 27 **LOS RIESGOS DE T.I.**

1.- Riesgos en la continuidad del proceso.- Cuando se refiere a riesgos en la continuidad del proceso, se involucran situaciones que pudieran afectar a la realización del trabajo informático o incluso que pudieran llegar a paralizarlo, y por consecuencia llegar a perjudicar gravemente a la empresa o incluso también a paralizarla. Ante los riesgos informáticos las empresas necesitan tomar precauciones con el fin de impedirlos, ninguna compañía está exenta de sufrir un percance que la afecte negativamente, ya sea un desastre natural o provocado por uno de los empleados.

- **Estrategias de Continuidad**

La continuidad de los servicios TI puede conseguirse bien mediante medidas preventivas, que eviten la interrupción de los servicios, o medidas reactivas, que recuperen unos niveles aceptables de servicio en el menor tiempo posible. Es responsabilidad de la Gestión de la Continuidad del Servicio diseñar actividades de prevención y recuperación que ofrezcan las garantías necesarias a unos costes razonables.

- **Actividades preventivas**

- Las medidas preventivas requieren un detallado análisis previo de riesgos y vulnerabilidades. Algunos de ellos serán de carácter general: incendios, desastres naturales, etcétera, mientras que otros tendrán un carácter estrictamente informático: fallo de sistemas de almacenamiento, ataques de hackers, virus informáticos, etcétera.

- La adecuada prevención de los riesgos de carácter general depende de una estrecha colaboración con la Gestión de la Continuidad del Negocio (BCM) y requieren medidas que implican a la infraestructura "física" de la organización.
- La prevención de riesgos y vulnerabilidades "lógicas" o de hardware requiere especial atención. En este aspecto es esencial la estrecha colaboración con la Gestión de la Seguridad.
- Los sistemas de protección habituales son los de "Fortaleza" que ofrecen protección perimetral a la infraestructura TI. Aunque imprescindibles no se hallan exentos de sus propias dificultades pues aumentan la complejidad de la infraestructura TI y pueden ser a su vez fuente de nuevas vulnerabilidades.

➢ **Actividades de recuperación**

- Tarde o temprano, por muy eficientes que seamos en nuestras actividades de prevención, será necesario poner en marcha procedimientos de recuperación.
- En líneas generales existen tres opciones de recuperación del servicio:
- COLD STAND BY: que requiere un emplazamiento alternativo en el que podamos reproducir en pocos días nuestro entorno de producción y servicio. Esta opción es la adecuada si los planes de recuperación estiman que la organización puede mantener sus niveles de servicio durante este periodo sin el apoyo de la infraestructura TI.
- WARM STAND BY: que requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas.
- HOT STAND BY: que requiere un emplazamiento alternativo con una replicación continúa de datos y con todos los sistemas activos preparados para la inmediata sustitución de la estructura de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales.

2.- Riesgos de la seguridad lógica.- Son todos aquellos accesos no autorizados a la información mecanizada mediante técnicas informáticas o de otros tipos. En cuanto a los riesgos de la seguridad lógica se mencionan los siguientes:

- Seguridad en el uso de software y los sistemas
- La protección de los datos, procesos y programas
- Acceso ordenado y autorizado de los usuarios a la información
- Así como la administración de usuarios y administradores de recursos de tecnología de información.[52]

Se tienen en cuenta las siguientes consideraciones, basados en la norma No 305-03 del Manual sobre Normas Técnicas de Control Interno Relativa a los Sistemas de Información Computarizados emitido por la Superintendencia de Bancos en el Ecuador la cual establece las acciones a considerar en cuanto a la seguridad lógica se refieren a :

- ➢ Restringir el acceso a programas y activos mediante claves y/o encriptación.
- ➢ Asignar las limitaciones correspondientes a cada usuario del sistema informático. Esto significa no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo.

[52] Plattini G. Mario y del Peso Emilio Op. Cit. Pág.572

- Asegurarse que los archivos y programas que se emplean son los correctos y se usan correctamente. Por ejemplo el mal uso de una aplicación puede ocasionar agujeros en la seguridad informática.
- Control de los flujos de entrada y salida de la información. Esto incluye que una determinada información llegue solamente al destino que se espera que llegue, y que la información llegue tal cual se envió.[53]

3.- Riesgos de seguridad física.- Se refiere a los controles y mecanismos de seguridad dentro y alrededor de las TI así como los medios de acceso remoto; implementado para proteger el hardware y medios de almacenamiento de datos. En general, en cuanto a la seguridad física, se debe tener en cuenta los riesgos asociados a:

- Acceso no autorizado a servidores y equipos
- Acceso no autorizado a edificios y salas
- Incendio: detección de humos y/o elevada temperatura
- Agua: escapes, goteras, inundación, etc.
- Interrupciones del suministro eléctrico
- Acondicionamiento de temperatura y humedad[54]

4.- Riesgos de factor humano.- Se refiere a aquellas posibilidades de usos inadecuados de la Información por los empleados. Se puede decir que el factor humano puede ser el eslabón más débil en toda la cadena de seguridad y se encuentra presente en todos los procesos relacionados con la seguridad. En todos los procesos informáticos y empresariales existe la implicación de factores humanos ya sea en la toma de decisiones como en los procesos mismos. Sin embargo, se presta una atención especial a los ataques externos que provocan daños más o menos cuantificables, cuando la mayoría de los incidentes ocurren dentro de la propia organización por un error humano, una errónea utilización de los medios de trabajo o por un ataque premeditado, falta de capacitación o la ausencia de una cultura de seguridad.

5.- Riesgos en la eficacia del servicio informático.- Son aquellos que alteren dicha realización o que afecten a la exactitud de los resultados ofrecidos por el servicio informático.

6.- Riesgos en la eficiencia del servicio informático.- Son los riesgos que se refieren a la mejor forma de realizar los procesos o trabajos, ya sea a nivel económico o técnico, pretendiendo con el análisis de estos riesgos mejorar la calidad del servicio.

7.- Riesgos económicos directos.- Se refiere a aquellas posibilidades de desembolsos directos Inadecuados.[55]**(Cuadro explicativo y sintetizado Ilustración No.27)**

[53] http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio/proceso_gestion_de_la_continuidad_del_servicio/organizacion_y_planificacion_de_la_continuidad_del_servicio.php

[54] www.cert.inteco.es

[55] www.siu.edu.ar

4.4.- CONCEPTOS BÁSICOS DE GESTIÓN DE RIESGOS DE T.I.

La gestión de riesgos es el proceso que permite a los administradores de TI equilibrar el funcionamiento y los costos económicos de las medidas de protección y conseguir mejoras en la capacidad de la misión por la protección de los Sistemas de TI y los datos que apoyan las misiones de sus organizaciones.

La gestión de riesgos es una piedra angular del gobierno de TI, asegurando que los objetivos estratégicos del negocio no son puestos en peligro por TI.

De acuerdo con el Marco COSO ERM, la gestión de riesgos empresariales abarca:

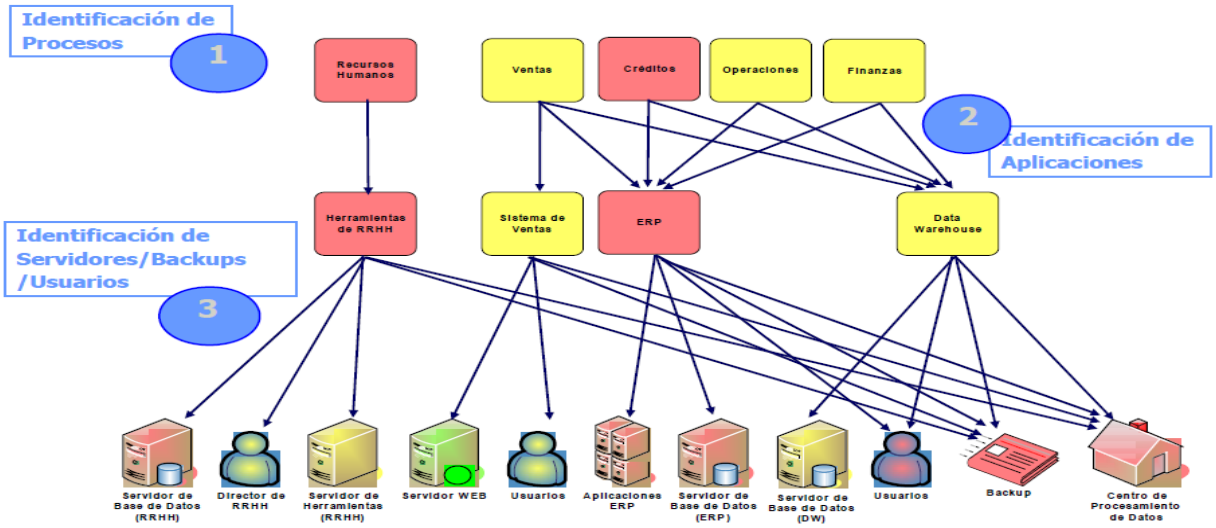
1. Alineación de apetito por el riesgo
2. Mejora la respuesta al riesgo
3. La reducción de sorpresas operacionales
4. Identificar y gestionar los riesgos múltiples y cruzar la empresa
5. Aprovechar las oportunidades
6. Mejorar la implementación del capital

Este proceso no es exclusivo del entorno de TI, de hecho domina la toma de decisiones en todos los ámbitos de nuestra vida cotidiana. Tomemos el caso de seguridad en el hogar, por ejemplo. Muchas personas deciden tener sistemas de seguridad instalados y pagar una cuota mensual a un proveedor de servicios para que estos sistemas de seguimiento para la mejor protección de su propiedad. Presumiblemente, los dueños de casa han pesado el costo de instalación del sistema y vigilancia contra el valor de los bienes de su hogar y la seguridad de su familia, un derecho fundamental.

Estos dueños de la misión debe determinar las capacidades de seguridad que sus sistemas de TI debe tener para proporcionar el nivel deseado de apoyo a la misión en el mundo real frente a la amenazas. La mayoría de las organizaciones tienen presupuestos limitados para la seguridad de TI, por lo tanto, la seguridad de TI el gasto debe ser revisado tan a fondo como las decisiones de gestión. Un riesgo bien estructurado dentro de la metodología de gestión es cuando se utiliza eficazmente y puede ayudar a identificar exactamente los riesgos que afectan directamente a los procesos de negocio y de esta forma establecer un sistema adecuado de controles para proporcionar las capacidades de seguridad esenciales para cumplir la misión del sector.

La gestión de riesgos comprende tres procesos: la evaluación de riesgos, mitigación de riesgos y evaluación. Según COSO “La evaluación del riesgos consiste en la identificación y análisis de los factores que podrían afectar la consecución de los objetivos, y, en base a dicho análisis, determinar la forma en que los riesgos deben ser gestionados”. Esta simple declaración es la base de la revolución del tratamiento de la gestión de riesgos, las metodologías de auditoría y la gestión del tema gobiernos corporativo**. (Véase Ilustración No.28)**

ILUSTRACIÓN 28 **PRINCIPALES PASOS EN UN ANÁLISIS DE RIESGO DE TI**



4.5.- PLANIFICACIÓN DE UNA OFICINA DE ADMINISTRACIÓN DE RIESGOS DE T.I.

La oficina de administración de riesgos de T.I. es de vital importancia dentro del funcionamiento del sector de mercado de valores, la práctica ha demostrado que la función de TI y los riesgos de TI, a menudo no son bien comprendidos por los principales de una organización, entre ellos los miembros de una junta y la dirección ejecutiva. Sin embargo, estas son las personas que dependen de TI para alcanzar los objetivos estratégicos y operativos de la organización y, en consecuencia, deberían ser los responsables de la gestión de los riesgos. Sin una clara comprensión de la función y de los riesgos asociados a TI, los ejecutivos de alto rango no tienen un marco de referencia para priorizar y administrar los riesgos de TI.

Los riesgos de TI no son puramente una cuestión técnica. A pesar de que se necesita de expertos en la materia para entender y gestionar los aspectos de los riesgos de TI, el conocimiento sobre la gestión del negocio es lo más importante. Los gerentes del negocio han de determinar lo que se debe hacer para apoyar su negocio y establecer los objetivos de TI. Por consiguiente, son responsables de la gestión de los riesgos asociados. En RISK IT, la gestión del negocio incluye los roles o cargos corporativos, líderes del negocio y funciones de apoyo (director financiero [CFO], jefe de información [CIO], recursos humanos [HR], etc.

La oficina de administración de riesgos de T.I., surge como una unidad responsable de la organización, coordinación y dirección del conjunto (portafolio) de riesgos identificados de la organización con la finalidad de mejorar el proceso de realización y los resultados de los objetivos del negocio.

Puede realizar funciones tácticas orientadas a la dirección de los riesgos críticos: creación y mantenimiento del proceso de realización, seguimiento de riesgos que afecten directamente la parte estratégica del mercado de valores, revisión, formación y apoyo a los gerentes de proyecto,

ejecución de acciones correctivas, realizan además las funciones que contribuyen a la estrategia de la organización, tiene un rol de soporte, de promotor de las mejoras.[56]

4.5.1. FUNCIONES DE LA OFICINA DE ADMINISTRACIÓN DE RIESGOS DE TI

1.- Establecer y aplicar las 3 disciplinas fundamentales para la gestión de riesgos en los servicios de T.I.

- Base: consolidada para disminuir riesgo, logrando la competencia
- Proceso de la gestión de riesgo, logrando la competencia
- Cultura de la concienciación del riesgo, considerando en este aspecto que la tecnología sólo puede ser realmente efectiva con la reducción de riesgos, entendiendo que la concienciación del riesgo se fomenta de arriba abajo.

  Para crear concienciación, es preciso segmentar el público e informar con frecuencia

  - Ejecutivos: concienciar en base al liderazgo y el status del programa
  - Directivos: concienciar en base a la integración y la ejecución
  - Profesionales de las TI: diseñar sistemas basados en la concienciación del riesgo.
  - Comunicación vertical continua
  - Preparar un plan de contingencia ante desastres

  Considerando que la cultura, las circunstancias y las aptitudes afectan a la disciplina focal:

  - La cultura organizativa
  - La Historia
  - El tamaño
  - La industria
  - La geografía
  - Las capacidades

2.- Sentar las bases: reforzar la base de la pirámide de riesgos en los servicios TI.- Consiste en una base tecnológica sólida, analizando los riesgos desde la base de la pirámide hacia arriba y principales factores de riesgo TI y la pirámide de riesgos TI, sentando las bases a partir de un proceso de tres fases. Desarrollar y poner a prueba un plan de continuidad empresarial. Dentro de este aspecto se debería:

- Gestionar los principales pasos para la continuidad del negocio en forma efectiva
- Análisis del impacto en el mercado de valores para establecer las prioridades y los plazos de recuperación, clasificando los niveles de servicios con sus respectivos riesgos.
- Desarrollar y ejecutar el plan de mitigación de riesgos.
- Identificar y corregir posibles fisuras, previendo desastres y realizando auditorías de TI
- Resultados conclusiones en la auditoría de seguridad y riesgos TI
- Promover controles y auditorías basados en marcos de trabajo estándar.
- Realizar las auditorías y revisiones.

[56] Risk IT, Framework, pag.11-12

- Soportar a proyectos en los riesgos inherentes
- Centralizar la información (repositorio)

3.- Implementar un proceso integral de gestión de riesgos TI efectivo y multicapa por medio de las fases que son:

- Definir estándares y políticas de control de riesgos
- Identificar y Evaluar los riesgos
- Priorizar los riesgos y asignar las responsabilidades
- Gestionar los riesgos
- Supervisar los riesgos y hacer el seguimiento.(Ciclo de Deming)
- Considerar las fuerzas externas nuevas o en proceso de cambio y analizar las iniciativas estratégicas, siempre incluyendo las tres disciplinas.

La implantación de las funciones de una Oficina de Gestión de Riesgos de TI normalmente pasa por varias etapas sucesivas que se fijan según las características y la madurez de la organización. En cada una de estas etapas se definen los objetivos, las funciones a implementar y los indicadores de seguimiento. Desde el punto de vista del equipo de implantación existen diferentes opciones:

Constituir un equipo formado por los recursos internos exclusivamente o crear un equipo mixto involucrando una empresa externa, preferiblemente independiente de los proveedores de Outsourcing y de desarrollo de proyectos.

El primer paso y la función de la Oficina de Gestión de Riesgos de TI, de vital importancia, establecer la metodología y el proceso de riesgos (proceso de producción) y promover su uso en la organización. El proceso definido fija el marco de referencia, la terminología común para todos los participantes y precisa los roles y responsabilidades de cada uno. En la definición de los procesos es conveniente utilizar los principios y los modelos estandarizados, tales como RISK IT, Cobit y especialmente ISO.-27005 por su orientación a la seguridad en la tecnología de información.

Las actividades de control y supervisión deben estar integradas con el proceso de realización. En este sentido las puntuales auditorías de TI (incluso de proyectos externalizados con los proveedores) por parte de la Oficina de Gestión de Riesgos. Toda esta información servirá de base para identificar tendencias, tomar acciones correctivas y obtener las previsiones de cumplimiento de los objetivos.[57]

4.5.2. CUADRO DE ROLES Y RESPONSABILIDADES DE LOS MIEMBROS DE UNA OFICINA DE ADMINISTRACIÓN DE RIESGOS DE TI.

En el cuadro se definen una serie de funciones para la gestión del riesgo y se indica que estas funciones asumen la responsabilidad o rendición de cuentas por una o más actividades dentro de un proceso.

La responsabilidad corresponde a aquellos que deben velar por que las actividades se completen con éxito y en su totalidad. La rendición de cuentas se aplica a quienes poseen los recursos necesarios y tener la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad específica dentro de los procesos de TI de riesgo. El cuadro que a continuación se detalla, es un resumen de los cuadros detallados en el modelo de proceso de una oficina de administración de riesgos de TI

[57] Consultoría Estratégica Conseti S.A., Mtro. Carlos Zamora, entrevista

La gráfica se desarrolla como parte del modelo de la administración de riesgos, en el cual se describen las etapas y sus responsables de ejecutar y así determinar el impacto (activos críticos y amenazas) y la probabilidad (vulnerabilidades y ambiente de control actual) para poder identificar el nivel de riesgo a que están expuestos los activos de tecnologías de información administrados por la Subdirección de Tecnología de la Información del mercado de referencia y con base en esto, ajustar o diseñar los controles para eliminar las vulnerabilidades y mitigar los riesgos. Derivado de la implementación de un marco de control interno y para maximizar los niveles de integridad, confiabilidad de la información, se realiza el proceso de administración de riesgos, mediante el cual se gestionarán los riesgos a los que están expuestos los activos de tecnologías de información institucionales administrados por la Subdirección de Tecnología de la Información, en la bolsa de valores del Ecuador.

Los requerimientos regulatorios a los cuales los responsables de la oficina de administración de riesgos deben de orientar sus funciones son:

- ISO 31000:2009- Lineamientos sobre los principios e implementación de la gestión de riesgos, www.iso.org.
- Guía de riesgos de los sistemas de tecnologías de información de NIST-publicación especial 800-30 www.nist.org
- Norma de gestión de riesgos AS/NZS 4360:2004- www.standards.com.au
- ISO 27005:2008- Administración de riesgos de seguridad informática www.iso.org.
- Risk IT Framework, www.isaca.org/riskfw- incluye una técnica de mapeo de riesgos, donde se puede identificar gráficamente el panorama general o específico (dependiendo de lo se desee proyectar en la gráfica) del análisis de riesgos realizado.

Las funciones descritas se aplican de manera diferente en cada organización. Para ello, cada función ha sido descrita brevemente en el cuadro. (**Ilustración No.29**)

ILUSTRACIÓN 29 **ROLES Y RESPONSABILIDADES DE LOS RESPONSABLES DE RIESGOS DE TI**

Responsabilidades y rendición de cuentas de los riesgos de TI											
Definición de la función		Gobierno del riesgo			Evaluación de riesgo			Respuesta de riesgo			
Función	**Definición sugerida**	**Visión común del riesgo**	**Integrar con ERM**	**Decisiones conscientes riesgo**	**Recopilar datos**	**Análisis del riesgo**	**Mantener el perfil de riesgo**	**Articular riesgo**	**Gestión de riesgos**	**Acontecimientos de riesgo**
Consejo	El grupo de los más altos ejecutivos y/o no-ejecutivos de la organización que son responsables de la gestión de la organización y tener el control total de sus recursos.									
(CEO) Director Ejecutivo	El más alto rango oficial que se encarga de la gestión total de la organización									
(CRO) Responsable de riesgos	Supervisa todos los aspectos de la gestión de riesgos en toda la organización. Un oficial de los riesgos, puede ser establecido para supervisar los riesgos relacionados con la TI									
(CIO) Responsable de TI	El más alto funcionario de la organización que es responsable de TI para la promoción, la alineación de TI y las estrategias organizacionales y la planificación, la asignación de recursos y la gestión de la prestación de los servicios de TI, la información y el despliegue de los recursos humanos asociados. El CIO normalmente preside el consejo de gobierno que maneja la cartera.									
(CFO) Responsable financier	El más alto funcionario de la organización que es responsable de la planificación financiera, el mantenimiento de registros, relaciones con los inversores y los riesgos financieros									
Comité de organización de riesgo	El grupo de ejecutivos de la organización que son responsables de la organización a nivel de la colaboración y el consenso necesario para apoyar las actividades de gestión de riesgos y decisiones. Un consejo de los riesgos puede ser establecido para examinar los riesgos con más detalle y asesorar al comité de organización de riesgo									
Gestión de Organización	Personas con funciones de negocio relacionadas con la gestión de un programa									
Propietario de procesos de negocio	La persona responsable de la identificación de los requisitos del proceso, diseño y proceso de aprobación de la gestión de proceso de ejecución. En general, un proceso de negocio debe ser titular en un nivel suficientemente elevado en la organización y tener autoridad para comprometer recursos para el proceso específico de las actividades de gestión de riesgo									
Funciones de control de riesgos	Las funciones en la organización responsable de la gestión de los dominios específicos de riesgo(por ejemplo el jefe de seguridad de la información oficial, la continuidad del negocio-plan de recuperación de desastres, la cadena de suministros, gestión de proyectos de oficina)									
(Rh) recursos humans	El más alto funcionario de una organización que es responsable de la planificación y las políticas con respecto a todos los recursos humanos en esa organización									
Cumplimiento y auditoria	La función en la organización responsable del cumplimiento y de auditoría									

Leyenda de la tabla:
Celda azul- El papel lleva la responsabilidad y/o rendición de cuentas parcial para el proceso
Celda roja- El papel lleva la responsabilidad principal de este proceso. Sólo un papel puede ser la principal responsable de un determinado
[58]

[58] Risk IT Pág. 19

4.5.3 BENEFICIOS Y RESULTADOS DE LA OFICINA DE ADMINISTRACIÓN DE RIESGOS DE TI

La oficina de administración de riesgos de TI, aborda muchas cuestiones a las cuales las organizaciones se enfrentan hoy en día. Es notable su necesidad ya que proporciona:

- Una visión precisa del presente y del futuro próximo sobre los riesgos relacionados con TI en toda la organización y el éxito con el que la organización se ocupa de dichos riesgos.
- Orientación de principio a fin sobre la forma de gestionar los riesgos relacionados con TI, más allá de medidas puramente técnicas de control y de seguridad.
- Comprensión de cómo capitalizar una inversión realizada en un sistema de control interno de TI ya existente para gestionar los riesgos relacionados con TI.
- En cuanto a la evaluación y gestión de los riesgos de TI, la integración con el riesgo global y el cumplimiento de las estructuras dentro de la organización.
- Establece un marco/lengua común mediante la guía del Risk IT, para ayudar a gestionar la relación entre los ejecutivos encargados de adoptar decisiones (o junta de los altos directivos), el director de información (CIO) y la organización de gestión del riesgo, o entre los auditores y la dirección.
- Promociona la responsabilidad del riesgo y su aceptación en toda la organización.
- Un perfil de riesgo completo para entender el riesgo y aprovechar mejor los recursos de la organización.

4.5.4 POLÍTICAS Y PROCEDIMIENTOS DE LA OFICINA DE ADMINISTRACIÓN DE RIESGOS DE TI

Como parte de la implementación de una oficina de control y gestión de riesgos de TI, las políticas son un conjunto de guías de acción que deberán aplicarse en el modelo de administración de riesgos de TI, sirviendo como soporte para la toma de decisiones, señalar responsables de su ejecución, delimitar alcances y plazos en la operación, precisar aspectos o casos de expedición en las actividades del procedimiento, así como completar con datos adicionales la descripción del procedimiento. Las políticas que se establezcan es aplicable de todos los responsables de los activos de tecnologías de información, que estén expuestos a las amenazas que pongan en riesgo los atributos de la información del mercado en estudio.

El ciclo de vida de las políticas consta de cuatro frases a) definición de la política; b) implementación de la política; c) verificación de su cumplimiento y d) revocación de la política, en el desarrollo de la presente tesis se definen las políticas que regirán el modelo de administración de riesgos tecnológicos, que representan el marco de referencia para la realización de las acciones que se deben emprender en un periodo de tiempo, en las cuales se incluye el “qué hacer”, “cómo hacerlo” y la “medida para evaluarlo”.

Las políticas del modelo de administración de riesgos definen las directrices para la gestión del riesgo, de manera que la entrega de servicios de TI se realice como lo requiere la institución; aseguran también que se cumplen las regulaciones, ayudan a la identificación de nuevos riesgos, proveen aseguramiento independiente de la entrega del valor de las tecnologías de información y la mitigación del riesgo.

Es por ello que las políticas que se han establecido en el presente documento, están dirigidas a los administradores o custodios de los activos de tecnologías de información institucionales, con la finalidad de establecer la rendición de cuentas, éstas políticas han sido dividas en tres responsables que se listan en seguida:

1. La Dirección de Tecnología y Desarrollo Institucional de la empresa dentro del mercado de valores ecuatoriano
2. La Subdirección de Tecnología de la Información de la entidad en referencia
3. El Grupo de trabajo de riesgos de tecnologías de información.

A continuación se presentan las políticas que se han definido para el modelo de administración de riesgos de TI:

1. La Dirección de Tecnología y Desarrollo Institucional será responsable de:
   1.1. Revisar y aprobar la directriz rectora del proceso de administración de riesgos de tecnologías de información, realizada por el Consejo Directivo de la Institución.
2. La Subdirección de Tecnología de la Información, será responsable de:
   2.1. Documentar y difundir una directriz rectora en donde se definan los antecedentes, sustentos y justificaciones de la necesidad de implantar la administración de riesgos tecnológicos en el Instituto, en conjunto con la Dirección de Tecnología y Desarrollo Institucional.
   2.2. Mantener el modelo de administración de riesgos de tecnologías de información, alineado con la estrategia de administración de riesgo de la Institución.
   2.3. Integrar el Grupo de trabajo de riesgos de tecnologías de información, para la realización del análisis y evaluación de riesgos sobre los activos de tecnologías de información institucionales, en el cual intervengan, los administradores o custodios de cada uno de los activos de tecnologías de información.
   2.4. Establecer y comunicar el alcance, objetivos, roles y responsabilidades de los integrantes del Grupo de trabajo de riesgos de tecnologías de información.
   2.5. Definir los reportes de gestión del proceso de Administración de riesgos de tecnologías de información, que de manera anual se elaborarán y comunicarán.
   2.6. Tomar decisiones de manera informada y oportuna sobre la mitigación de los riesgos asociados con las tecnologías de información institucionales a su cargo.

3. La Subdirección de Tecnología de la Información a través del Grupo de trabajo de riesgos de tecnologías de información, será responsable de:

3.1. Recopilar los datos relevantes relacionados con los riesgos en los activos de tecnologías de información institucionales, tales como:

3.1.1. Incidentes que hayan tenido algún impacto en la Institución.

3.1.2. Riesgos del activo de tecnologías de información institucionales a evaluar.

3.1.3. Controles actualmente implementados en los activos o recursos a evaluar.

3.2. Identificar y clasificar las amenazas y riesgos en el ambiente interno y externo, que podrían influir en los activos de tecnologías de información institucionales.

3.3. Identificar y analizar escenarios de riesgo en los activos de tecnologías de información institucionales, que permitan evaluar y obtener los impactos potenciales; para cada escenario de riesgo, definir y acordar la prioridad para su implantación.

3.4. Integrar las matrices de riesgo en los activos de tecnologías de información institucionales.

3.5. Identificar el nivel de severidad del riesgo.

3.6. Identificar opciones para el tratamiento y control del riesgo.

3.7. Identificar acciones preventivas, correctivas y correlacionarlas para cada uno de los escenarios de riesgos identificados.

3.8. Definir programas de mitigación del riesgo, los cuales considerarán las acciones para implantar los controles de riesgos en las Declaraciones de aplicabilidad.

3.9. Definir un Programa de contingencia para hacer frente a los eventos o incidentes de los riesgos identificados de tecnologías de información que pudieran presentarse.

3.10. Informar a las áreas normativas usuarias de las tecnologías de información institucionales, sobre los riesgos a los que se encuentran expuestos los procesos y servicios que utilizan.

3.11. Generar de manera semestral el indicador de cumplimiento de la administración de riesgos de tecnologías de información.

Estas son solo unas de las principales políticas que deben implementarse dentro de la Institución del mercado de valores las mismas que deben de ir acompañadas de una cultura de riesgos que ofrezcan un entorno en el que los componentes de riesgo se puedan discutir abiertamente y los niveles de riesgo aceptables se entiendan y se mantengan. La cultura de riesgos aceptables debe de comenzar desde la parte superior con la junta y los ejecutivos de negocios que establece la dirección, comunicando el riesgo de toma de decisiones aceptables y premiando la cultura de aprendizaje en la gestión eficaz del riesgo.

La cultura del riesgo incluye:

- El comportamiento hacia la toma del riesgo - ¿Cuál es el grado de riesgo que siente la organización que puede asumir y qué riesgos está dispuesta a tomar?
- El comportamiento hacia la política siguiente - ¿En qué medida la gente va a aceptar y / o cumplir con la política?

- El comportamiento hacia resultados negativos – ¿Cómo la organización se ocupa de los resultados negativos, es decir, acontecimientos de pérdida u oportunidades perdidas? ¿Aprenderá ellos de esto y tratarán de adaptarse, o se culpará sin tratar la causa de origen?

4.6.- MODELO INTEGRAL DE ADMINISTRACIÓN DE RIESGOS DE T.I.

El modelo integral de administración de Riesgos de TI es realizar un análisis, identificación y evaluación de riesgos a los que está expuesta normalmente una empresa, por lo que, una de nuestras finalidades y objetivos es proteger sus activos de la mejor manera posible y crear un programa de seguridad óptimo y adecuado al mercado de valores ecuatoriano.

Como parte de la implementación de un marco de control interno para maximizar los niveles de integridad, confiabilidad y seguridad de los datos e información se requiere la instrumentación de un proceso de administración de riesgos, que gestione los riesgos a los que están expuestos los activos de Tecnología de Información (TI) pertenecientes a la Subdirección de Tecnología de la Información (STI) de la Institución. Establecer y definir los procesos a seguir para efectuar la administración de riesgos de los activos de TI (hardware, software, información, infraestructura) de la STI.

Para ello, se desarrolló un modelo de administración de riesgos, el cual se detalla en este documento donde se describen cada una de las fases y etapas que conforman dicho modelo, con el objetivo de determinar el impacto (activos críticos y amenazas) y la probabilidad (vulnerabilidades y ambiente de control actual) para poder identificar el nivel de riesgo a que están expuestos los activos de TI y con base en esto se ajustan o diseñan controles para eliminar las vulnerabilidades y mitigar los riesgos.

El modelo de la Administración de Riesgos a implementar en la STI (Subdirección de Tecnologías de Información) cuenta con las siguientes etapas: **(véase Ilustración No.30)**

ILUSTRACIÓN 30 **MODELO INTEGRAL DE ADMINISTRACIÓN DE RIESGOS A IMPLEMENTAR EN LA SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN DE UNA INSTITUCIÓN DEL MERCADO DE VALORES ECUATORIANO**

4.6.1.- FASE 1.- ANÁLISIS Y EVALUACIÓN

El análisis y evaluación de riesgos sobre activos de TI debe realizarse por un grupo interdisciplinario coordinado por un representante de la función de seguridad de TI. En este grupo deberán intervenir, por lo menos, el dueño y los administradores o custodios de cada uno de los activos de TI pertenecientes a la STI. Dentro de esta fase las etapas a cumplir son:

4.6.1.1.- Análisis de procesos

Identificar y mapear los principales procesos de las áreas clave de la STI, realizando las siguientes actividades:

- Determinar objetivo, entradas y salidas de cada proceso.
- Identificar principales actores.
- Delimitar los procesos (fronteras de responsabilidad).
- Identificar los principales flujos de información.

4.6.1.2.- Clasificación de los riesgos

La identificación del activo y de sus componentes es el primer paso para el desarrollo de un análisis de riesgos. Identificando únicamente los activos críticos.

Para la clasificación de los activos de TI se debe considerar la importancia de la información que es almacenada, procesada o transmitida por dicho activo; por ejemplo, si un servidor procesa información clasificada como crítica, entonces el servidor será considerado como crítico.

Todos los activos de TI administrados por la STI, deben ser clasificados por su dueño considerando las siguientes propiedades:

- Confidencialidad: Garantizar que la información será accedida únicamente por personal autorizado.
- Integridad: Garantizar que la información será modificada únicamente por personal autorizado.
- Disponibilidad: Garantizar que la información estará disponible en el momento que sea requerido por el personal autorizado y para los fines que fue creada.

4.6.1.2.1. - NIVELES DE CLASIFICACIÓN DE ACTIVOS DE TI

La siguiente tabla muestra los niveles de clasificación de los activos de tecnología de información y la descripción de cada uno de ellos. (**Véase Ilustración No.31)**

ILUSTRACIÓN 31 **NIVELES DE CLASIFICACIÓN DE ACTIVOS DE TI**

PROPIEDAD	NIVEL DE CLASIFICACIÓN	DESCRIPCIÓN
Confidencialidad	C1 - Pública	No requiere restricciones de acceso. La divulgación de esta información, no impacta negativamente a la Institución
	C2 – Confidencial	Acceso restringido a un número determinado de usuarios. La divulgación no autorizada de esta información podría impactar desde una persona o hasta varias áreas de la Institución Aplica a información personal.
	C3 - Reservada	El acceso a esta información debe ser estrictamente restringido. La divulgación no autorizada de esta información

PROPIEDAD	NIVEL DE CLASIFICACIÓN	DESCRIPCIÓN
		podría impactar seriamente a la Institución. Aplica a los activos de información más sensitivos.
Integridad	I1 - Estándar	No requiere control de acceso para restringir modificaciones. La modificación no autorizada de información no tiene un impacto significativo.
	I2 – Individual	Requiere de restricciones individuales para su modificación. La modificación no autorizada de esta información podría impactar a una persona o varias áreas del Instituto.
	I3 - De doble intervención	Requiere necesariamente que dos personas den su autorización para poder realizar modificaciones. La modificación no autorizada de esta información podría impactar seriamente al Instituto. Aplica a los activos de información más sensitivos.
Disponibilidad	D1 - Recuperable	Prescindir del activo por más de un día, no impacta seriamente a la Institución En caso de contingencia grave, se puede esperar hasta 72 horas hábiles[59] para recuperar el activo.
	D2 - Altamente recuperable	Prescindir del activo por un día o más, impactaría seriamente al Institución. En caso de contingencia grave el activo debe recuperarse en menos de 24 horas hábiles.
	D3 - Alta disponibilidad	Cero tolerancias a interrupciones o fallas, prescindir de este activo afectaría gravemente a la Institución.

[59] Se consideran 8 horas hábiles por día.

4.6.1.3.- IDENTIFICAR AMENAZAS

Una amenaza es toda aquella situación o evento, ya sea interno o externo, que puede comprometer la seguridad de un activo.

Una vez clasificado el activo es indispensable identificar las amenazas a las que se encuentra sujeto.

Por ejemplo, amenazas a las que se encuentra expuesto un servidor de correo electrónico:

- Código malicioso
- Acceso no autorizado
- Ataques de negación de servicio

4.6.1.4.-IDENTIFICAR VULNERABILIDADES

Una vulnerabilidad es una característica propia del activo que lo hace susceptible de ataques o débil ante la materialización de una amenaza.

Las vulnerabilidades deben estar relacionadas directamente con el activo. Por ejemplo, vulnerabilidades que pueden pertenecer a un servidor de correo electrónico:

- Falta de actualizaciones (parches).
- Configuración inadecuada de seguridad.
- Deficiente soporte técnico del fabricante.

Cabe mencionar dentro de este apartado la metodología NIST donde se encuentra una base de datos actualizada de una serie de vulnerabilidades entre las que podemos citar los más representativos para el negocio por ejemplo: CVE-2010-3600 permite a atacantes remotos afectar a la confidencialidad, integridad y disponibilidad a través de vectores desconocidos, CVSS: gravedad:7,5(Alto). [60]

En el capítulo 6 analizaremos de una manera más práctica la aplicación de esta metodología.

4.6.1.5.- IDENTIFICAR OCURRENCIAS

Es necesario determinar la probabilidad de que una amenaza explote una característica de vulnerabilidad del activo y se materialice el riesgo convirtiéndose en una pérdida o daño para el Instituto, es muy importante que el administrador o dueño del activo determine la probabilidad de ocurrencia con base en los antecedentes e historia del activo dentro de la Institución, es decir, debe determinar el número de ocasiones en que se han materializado las amenazas explotando una o varias vulnerabilidades del activo originando la materialización del riesgo.

[60] http://web.nvd.nist.gov/view/vuln/search-results?query=vulnerability+of+data+base&search_type=all&cves=on

La siguiente tabla ha sido diseñada para clasificar la probabilidad, con base en la frecuencia de ocurrencias identificadas por los administradores o dueños del activo; en caso de que no se cuente con información de incidencias pasadas, se deberá clasificar en base a estadísticas disponibles en el mercado.**(véase Ilustración No.32)**

ILUSTRACIÓN 32 IDENTIFICAR CATEGORIAS DE NIVEL DE OCURRENCIA

CATEGORÍA	DESCRIPCIÓN
Raro	En promedio menos de una ocurrencia anual
Poco Probable	En promedio una ocurrencia anual
Probable	En promedio dos ocurrencias anuales
Muy Probable	En promedio doce ocurrencias anuales
Seguro	En promedio más de doce ocurrencias anuales

4.6.1.6.- IDENTIFICAR IMPACTO

Impacto es el efecto adverso resultante de una amenaza que se materializó, motivo de una o varias vulnerabilidades.

Por ejemplo, el impacto de un virus que se materializó a través de una vulnerabilidad en el servidor de correo electrónico, es el siguiente:

- Daños o pérdida de Información.
- Interrupción de las operaciones.
- Pérdidas indirectas como consecuencia de daño a la reputación e imagen de la Institución

Una vez realizada la clasificación del activo e identificadas las amenazas a las que está expuesto, se determina el nivel de impacto que puede representar para la Institución la pérdida o daño del activo.

Para determinar el nivel de impacto se ha definido una clasificación con cinco categorías, como sigue:

- Insignificante
- Menor
- Moderado
- Mayor
- Catastrófico

El impacto puede ser evaluado de forma financiera, de imagen, legal u operacional. Como ejemplo se presenta la siguiente tabla:

ILUSTRACIÓN 33 **IDENTIFICAR CATEGORÍAS DE IMPACTO DE LOS RIESGOS DE SEGURIDAD DE TI**

CATEGORÍA	AFECTA SERVICIOS PROPORCIONADOS POR LA STI	AFECTACIÓN A USUARIOS	PERCEPCIÓN / DAÑOS
Insignificante	NO	Afecta a una sola persona	No hay daños perceptibles para la STI o cualquier otra área.
Menor	SI	Afecta a un grupo menor de personas	El incidente causa un daño reparable de menor importancia, es perceptible para la STI.
Moderado	SI	Afecta a gran parte de una Jefatura de Servicios	El incidente causa un daño reparable y es perceptible para la Dirección de Finanzas de la Institución.
Mayor	SI	Afecta a gran parte de una Dirección	Daño severo a los procesos o a la capacidad de alcanzar las metas del plan estratégico de la Institución.
Catastrófico	SI	Afecta a gran parte de la Institución	El daño es perceptible por clientes, socios, proveedores o sociedad en general. El incidente puede poner en peligro vida humana.

Es posible que algunas vulnerabilidades que se identifiquen ya estén cubiertas por controles anteriormente implementados, por lo cual se deberá hacer un análisis de dichos controles para confirmar si pueden ser descartadas o no del análisis de riesgos. **(Véase Ilustración No.33)**

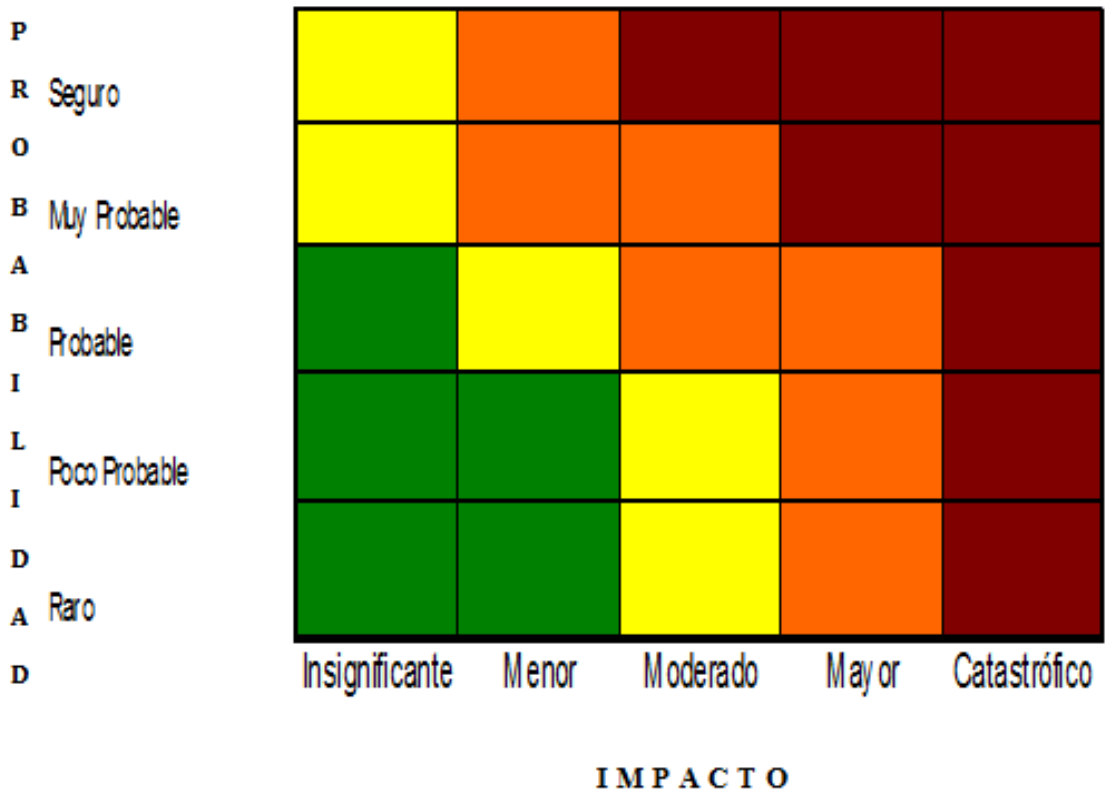
4.6.1.7.- CALIFICAR CUALITATIVAMENTE

Para la clasificación del riesgo se han definido cuatro categorías que corresponden a las siguientes equivalencias: **(véase Ilustración No.34)**

Verde	Bajo
Amarillo	Menor
Naranja	Moderado
Rojo	Alto

La clasificación del riesgo se obtiene ubicando el impacto y la probabilidad en la siguiente tabla:

ILUSTRACIÓN 34 **CLASIFICACIÓN DEL RIESGO DE ACUERDO A SU IMPACTO Y PROBABILIDAD**



4.6.1.8.- CALIFICAR CUANTITATIVAMENTE

Para poder calcular el valor cuantitativo de los riesgos se requiere:

1. Estimar la pérdida potencial considerando el valor del activo.
2. Analizar las amenazas potenciales sobre el activo.
3. Determinar la expectativa anualizada de pérdida.

Para determinar la expectativa anualizada de pérdida (ALE) es necesario realizar los siguientes pasos:

1. Determinar la expectativa de pérdida por evento (SLE)

   SLE = Valor del activo ($) x Factor de exposición (EF)

   Dónde:

   SLE: Figura monetaria que se le asigna a un evento.

   Valor del activo ($): Valor monetario del activo para la Institución

   Factor de exposición (EF): Porcentaje de pérdida que una amenaza podría representar sobre un activo específico.

2. Determinar expectativa anualizada de pérdida (ALE)

   ALE = SLE x Tasa de ocurrencia anualizada (ARO)

   Dónde:

   ALE: Figura monetaria que representa la expectativa de pérdida anual.

   ARO: Número que representa la frecuencia estimada en la cual una amenaza se podría presentar.

Nota: En caso de no poder realizar una valoración cuantitativa deberá tomarse solamente la calificación cualitativa considerando el número de ocurrencias anuales (ARO) y el factor de exposición del activo (EF) en la toma de decisiones.

4.6.2.- FASE 2.- TOMA DE DECISIONES

Es importante tener presente la relación de riesgo - beneficio, en cualquier decisión que se tome con respecto a la solución que se le va dar al riesgo para ser tratado. Tomando en consideración una estrategia de control, donde se adopten métodos y medidas para salvaguardar los activos administrados por la STI, con el fin de maximizar los niveles de integridad, confiabilidad y seguridad de los datos e información de la Institución. Las etapas que se desarrollan en esta fase son:

4.6.2.1.- TRATAMIENTO DE RIESGOS

Con la finalidad de incluir solamente riesgos que impacten a la Institución, serán únicamente seleccionados los riegos moderados y altos en el proceso de administración de riesgos.

Análisis costo-beneficio

Se entiende por análisis del costo-beneficio al balance entre el costo de implantación de las medidas de control para salvaguardar los activos administrados por la STI, contra la no materialización de los riesgos analizados anteriormente.

El criterio de costo-beneficio toma en cuenta la posibilidad de ocurrencia de daños materiales y la reparación de los mismos.

Para determinar el análisis de riesgos, se debe tomar en cuenta lo siguiente, con el fin de tener un eficaz gobierno sobre la gestión de riesgos de TI:

- El riesgo es prioridad y se debe dirigir en base al apetito y la tolerancia que la STI tiene hacia el riesgo.
- Los controles deben ser aplicados para hacer frente a un riesgo basándose en un análisis costo-beneficio.

4.6.2.2.- DETERMINAR ACCIÓN VS RIESGO

Se debe definir una acción o respuesta a cada uno de los riesgos encontrados después del análisis, de acuerdo con la tolerancia al riesgo dentro de la STI. Las opciones para dar respuesta al riesgo son: mitigar, transferir y aceptar; dependiendo de la decisión que se tome con respecto a la acción se definen las actividades que complementan el tratamiento a los riesgos identificados.

La selección de una respuesta adecuada, al riesgo dado, se deben tenerse en cuenta lo siguiente:

- Costo de la acción para dar tratamiento al riesgo.
- Importancia del riesgo dirigida por la respuesta, es decir, el reflejo de la frecuencia y los niveles combinados con la magnitud del riesgo.

4.6.2.3.-ESTABLECER ESTRATEGIA DE CONTROL

Después de determinar las acciones a seguir para dar respuesta a los riesgos identificados, es importante identificar y/o establecer una serie de medidas de control, destinadas a reducir la frecuencia de un evento y/o el impacto hacia la institución.

Estas actividades de control comúnmente son conocidas como controles de TI, los cuales son de dos tipos:

Controles a nivel estratégico:

- Definición de la estrategia de TI.
- Selección de Arquitectura de TI.
- Establecimiento de políticas y procedimientos de gestión de recursos humanos, entre otros.

Controles Generales de TI

- Controles de funcionamiento del centro de datos como políticas y procedimientos de configuración, de operación, de respaldo y recuperación de datos.
- Controles de software como adquisición y ejecución de software, desarrollo y mantenimiento, metodología de desarrollo, gestión del cambio, administración de la base de datos.

- Controles de seguridad como son los controles de acceso que impiden el uso inapropiado y no autorizado a los activos de TI.
- Controles de Administración de TI e Infraestructura.

4.6.2.4.- IDENTIFICAR POLÍTICAS Y PROCEDIMIENTOS

Es necesario identificar aquellas políticas y procedimientos que sean necesarios dentro de la STI como parte de la estrategia de control que se definió con anterioridad.

A través de entrevistas y revisión de documentación se deben identificar los controles implementados que apoyen a minimizar el riesgo. Deberá identificarse:

- Control
- Responsable
- Descripción
- Tipo (Preventivo / Detectivo)
- Frecuencia

Adicionalmente deberá revisarse la evidencia que asegure que el control se encuentra en operación.

En caso de no existir controles que apoyen a minimizar el riesgo identificado, deberán diseñarse los controles correspondientes, incluyendo la justificación del control. Dichos controles deberán documentarse en las políticas y procedimientos de la STI.

A continuación se enlistan algunos ejemplos de las políticas que se pudieran implementar posteriormente.

- Políticas y procedimientos de Operación y Administración de TI.
- Atención a usuarios
- Uso y aprovechamiento del software y hardware institucional
- Administración de bases de datos
- Control de cambios
- Administración de problemas e incidentes
- Administración de proyectos
- Políticas y procedimientos de Desarrollo, Mantenimiento y Soporte.
- Desarrollo de Sistemas
- Administración de requerimientos de software
- Control de versiones
- Políticas y procedimientos de Seguridad.
- Autenticación y control de accesos
- Respaldo y restauración de información
- Monitoreo de operaciones

4.6.2.5.- IDENTIFICAR TÉCNICAS Y METODOLOGÍAS

Se debe realizar un análisis para poder identificar aquellas técnicas y metodologías que se van a utilizar durante el proceso de administración de riesgos dentro de la STI de acuerdo a sus necesidades, por ejemplo:

- ISO 31000:2009 – Lineamientos sobre los principios e implementación de la gestión de riesgos (se encuentra en desarrollo) www.iso.org.
- Guía de riesgos de sistemas de tecnologías de información de NIST, publicación especial 800-30 www.nist.org
- Norma de gestión de riesgos AS/NZS 4360:2004 www.standards.com.au
- ISO 27005: Gestión de seguridad de la información www.iso.org.
- RISK IT Framework www.isaca.org/riskfw, incluye una técnica de mapeo de riesgos, donde se puede identificar gráficamente el panorama general o específico (dependiendo de lo que se desee proyectar en la gráfica) del análisis de riesgos realizado.

4.6.2.6.-ESTABLECER INDICADORES

Los indicadores clave de riesgo (KRI Key Risk Indicator) son las métricas que puedan demostrar que la institución está sujeto, o tiene una alta probabilidad de ser sometidos a un riesgo que excede su apetito al riesgo.

Para la identificación de los KRI debe tener en cuenta los siguientes aspectos (entre otros):

- Tener en cuenta las distintas partes interesadas en la Institución. Los KRI´s no deben centrarse únicamente en lo más operativo o en la parte más estratégica del riesgo. Pueden y deben ser identificados para todas las partes interesadas.
- Hacer una selección equilibrada de los indicadores de riesgo, que abarca los indicadores de desempeño (con indicación de qué capacidades están en su lugar para evitar que se produzcan acontecimientos) y las tendencias (análisis de indicadores en el tiempo o la correlación de los indicadores para obtener información).
- Asegúrese de que los indicadores seleccionados, los detalles de la causa raíz de los acontecimientos (indicativo de la causa raíz y no sólo los síntomas).

4.6.2.7.- ESTABLECER LÍMITES

Una vez establecidos los indicadores clave de riesgo, es importante que se establezcan los límites de cada uno de los KRI´s, con el fin de facilitar la evaluación y seguimiento de la administración de riesgos.

Por ejemplo:

KRI: Porcentaje de solicitudes de acceso no autorizadas al mes.

Métrica: Número de solicitudes no autorizadas / Número de solicitudes realizadas durante el mes = % solicitudes no autorizadas al mes.

Límite: 5 %

Esto significa que si se excede el límite del 5%, el nivel de riesgo es alto y se deberá tomar una acción de inmediato.

4.6.3.- FASE 3.- IMPLEMENTAR MEDIDAS DE CONTROL

El siguiente paso es implementar las medidas necesarias para garantizar el despliegue eficaz de los nuevos controles y ajustes de los controles existentes, para después comunicarlas a todo el personal clave que participa activamente en el proceso de administración de riesgos.

4.6.3.1.- DEFINIR FUNCIONES

Una de las actividades para empezar a implementar las medidas de control, es la definición de funciones para la administración de riesgos.

Se deben establecer los roles y responsabilidades que tiene cada una de las personas que participan en el proceso, así como la rendición de cuentas para una o más actividades dentro del mismo.

La rendición de cuentas se aplica a aquellos poseen los recursos necesarios y tienen la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad de riesgo específicos de los procesos de TI.

Es importante que la segregación de funciones este bien definida para que no exista conflicto de intereses entre las áreas.

Por ejemplo la NIST sugiere los siguientes roles y responsabilidades con respecto a la gestión de riesgos:

- Consejos de dirección y alta dirección de gobierno.
- Director de información
- Gerente de seguridad de la información
- Propietarios de sistemas e información
- Gerentes de negocio y operativos
- Profesionales de seguridad de TI
- Capacitación en concientización sobre la seguridad (profesionales en el tema seguridad)

4.6.3.2.- IMPLEMENTAR POLÍTICAS

Una vez definidas las funciones se debe comenzar a implementar las políticas que fueron definidas con anterioridad de acuerdo a las necesidades que tiene la STI.

4.6.3.3.- IMPLEMENTAR PROCEDIMIENTOS

Los procedimientos ya identificados pueden ser implementados a la par que las políticas, todo esto basándose en mejores prácticas y estándares internacionales.

4.6.3.4.- INSTRUMENTAR MECANISMOS DE MONITOREO Y CONTROL

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados

de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

4.6.3.5.- DEFINIR RESPUESTA A INCIDENTES

Es primordial prepararse a dar respuesta a incidentes, por lo que se debe definir las medidas específicas a tomar cuanto un evento de riesgo puede provocar un funcionamiento inadecuado de algún activo, y/o puede generar un impacto a la Institución.

Se debe mantener abierta la comunicación sobre la aceptación de riesgos, actividades de la administración de riesgos, técnicas de análisis y los resultados disponibles para ayudar con la definición de las medidas que darán respuesta a incidentes.

Es importante considerar cuánto tiempo el Instituto puede estar expuesto y cuánto tiempo puede tardar en recuperarse.

4.6.3.6.- COMUNICAR Y EDUCAR

La comunicación de riesgos es una parte clave en este proceso, se refiere a la idea de que para la gente es naturalmente incómodo el hablar de riesgo.

Las personas tienden a posponer la admisión de que el riesgo está implicado y comunicar acerca de cuestiones, los incidentes y, eventualmente, incluso crisis.

Tomar conciencia del riesgo es reconocer que el riesgo es una parte integral de la Institución. Esto no implica que todos los riesgos que deben evitarse, sino que los riesgos sean bien conocidos e identificables; y el Instituto reconoce y utiliza los medios para manejarlos.

4.6.4.- FASE 4.- MEDICIÓN Y SEGUIMIENTO

Como último paso del proceso de administración de riesgos se encuentra la medición y el seguimiento. Donde es importante vigilar cuando un límite de control ha sido violado, es decir cuando la medición del riesgo rebasa el límite pre-definido.

Se debe categorizar los incidentes (por ejemplo, la violación de la política, el fracaso del sistema, el acceso no autorizado, la demanda), y comparar las exposiciones reales contra umbrales aceptables; para que posteriormente sean comunicados los impactos institucionales al personal involucrado para una adecuada toma de decisiones; para así garantizar clara responsabilidad por las acciones de seguimiento.

4.6.4.1.- ESTABLECER BASE DE DATOS HISTÓRICA

El registro de riesgo es una técnica de guardar y mantener toda la información recopilada en un formato útil para todos aquellos interesados.

El registro de riesgo puede ser visto como una extensión del mapa de riesgos, proporcionando información detallada sobre cada riesgo identificado incluyendo:

- Información sobre el dueño de riesgo.
- Información sobre los detalles del escenario del riesgo.
- Información sobre resultados detallados en el análisis de riesgo.
- Información detallada sobre la respuesta a los riesgos y el estado de respuesta a los mismos.
- Información sobre los controles existentes.

El registro de riesgo sirve como la principal referencia para todos los riesgos relacionados con la información, el apoyo a todos los riesgos relacionados con las decisiones.

4.6.4.2.- EVALUACIÓN DEL PROCESO

Una vez que esté implementada la estrategia de control para la administración de riesgos, se debe realizar una evaluación formal de todo el proceso que requiere el modelo de administración de riesgos como tal, tomando en consideración mecanismos de retroalimentación de todo el personal involucrado en dicho proceso. Todo esto con el fin de tener una mejora continua cumpliendo con los objetivos de la Institución.

4.6.4.3.- VERIFICAR PROCESOS DE MONITOREO Y CONTROL

Después de establecer un programa de control interno efectivo para TI y el proceso de monitoreo, es primordial darle seguimiento y verificar que dicho programa está cumpliendo su objetivo, reportando las excepciones de control, lo resultados de las auto-evaluaciones y revisiones por parte de terceros.

4.6.4.4.- REVISIÓN A LOS DATOS Y REGISTROS

En la revisión a los datos y registros es importante examinar los últimos acontecimientos adversos, oportunidades y pérdidas.

Se debe determinar si hubo una falla derivada de la falta de conciencia, la capacidad o de motivación para después investigar la causa raíz de los eventos de riesgo similar y la eficacia relativa de las medidas adoptadas entonces y ahora.

Se debe dar un monitoreo continuo a los datos y registros para poder identificar la causa raíz de los problemas e incidencias de eventos.

4.6.4.5.- EVALUACIÓN DE SEGURIDAD

El objetivo de la seguridad de la información es proteger los intereses de aquellos que dependen de todos los activos de Tecnología que proporcionan la información de los daños resultantes de los fracasos de la disponibilidad, confidencialidad e integridad.

Es importante evaluar cuando menos que:

- Todos los activos de Tecnología de estén disponibles y utilizables cuando se requiera, y tengan una adecuada resistencia a los ataques se puedan recuperar de los fracasos (disponibilidad).
- La información sea observada o revelada sólo a aquellos que tienen derecho a saber (confidencialidad).
- La información está protegida contra la modificación no autorizada (integridad).

4.6.4.6.- AUDITORÍA INTERNA

La auditoría interna es la revisión del funcionamiento de la operación, administración y seguridad de TI por personal de la misma STI, donde se toman las deficiencias y los riesgos para la Institución; ayudando a los involucrados a entender los planes de acción correctiva cómo afectará el riesgo global de perfil. Todo esto con el fin de poder identificar oportunidades para la integración con los esfuerzos de rehabilitación y otras actividades de la administración de riesgos en curso.

4.6.4.7.- AUDITORÍA EXTERNA

En la auditoría externa se deben considerar los resultados de la evaluación independiente que tuvo el área de TI (en este caso la STI), donde el personal involucrado revisa los resultados y conclusiones específicas de entes externos, con el fin de que se evalúe y verifique el funcionamiento correcto de la operación, administración y seguridad de TI dentro de STI, para poder determinar el cumplimiento de la estrategia de control y ver si los riesgos son tratados adecuadamente.[61]

[61] Consultoría Estratégica Conseti S.A., Mtro. Carlos Zamora, entrevista

4.7.- AUDITORÍA BÁSICA DE UNA ADMINISTRACIÓN DE RIESGOS ASOCIADAS A LAS T.I.

4.7.1. AUDITORÍA EN T.I.

La sociedad actual se dirige a vivir en lo que se denomina aldea global, suceso que evoluciona al género humano en múltiples direcciones, en especial lo referente a las TI. Por lo tanto, la auditoría debe ser consecuente con tales transformaciones para integrarlas en su campo de acción y transmudarse, adaptándose a los diferentes cambios económicos y de mercado, para convertirse en motor de innovación y cambio en pro del mejoramiento continuo en las organizaciones, respondiendo así a las necesidades de la futura aldea global.

4.7.1.1. CONCEPTO DE AUDITORÍA

La auditoría es la investigación, consulta, revisión, verificación, comprobación y evidencia aplicada a la empresa. Es el examen realizado por el personal calificado e independiente de acuerdo con Normas de Contabilidad, con el fin de esperar una opinión que muestre lo acontecido en el negocio, requisito fundamental es la independencia.

También se define como la actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones, estándares y otros requisitos, la adhesión a los mismos y la eficacia de su instrumentación.

Otra definición proporcionada por Mario Plattini dice que auditoria es la emisión de una opinión profesional sobre el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y cumple las condiciones que le han sido prescritas.

4.7.1.2. CONCEPTO DE AUDITORIA EN T.I.

La auditoría en T.I. es una extensión del auditor tradicional, puede definirse como la revisión analítica a la suficiencia de controles establecidos en el ámbito informático con la finalidad de disminuir los riesgos y garantizar la seguridad, confiabilidad y exactitud de la información.

Por otra parte, auditoría en TI también se define como el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático en la empresa por lo que comprende un examen metódico puntual y discontinuo del servicio informático con vistas a mejorar en rentabilidad, seguridad y eficacia.

Para efecto de la presente tesis se toma el concepto de auditoría en TI salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza

eficientemente los recursos. De este modo la auditoría en informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos
- Objetivos de gestión que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia.

4.7.1.3 TIPOS DE AUDITORÍA EN T.I.

Dentro de la auditoría en TI destacan los siguientes tipos.

- Auditoría de la gestión: Retenido a la contratación de bienes y servicios, documentación de los programas, etc.
- Auditoría legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- Auditoría de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los diagramas de flujo.
- Auditoría de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.
- Auditoría de la seguridad: En relación a los datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- Auditoría de la seguridad física: Con respecto a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, vigilantes, etc.) y protecciones del entorno.
- Auditorías de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.
- Auditoría de las comunicaciones: Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes.

Diferentes acepciones de auditoría en TI

- Auditoría en informática como soporte a la auditoría tradicional, financiera, etc.
- Auditoría en informática con el concepto anterior, pero añadiendo la función de auditoría de la función de gestión del entorno informático.
- Auditoría en informática como función independiente, enfocada hacia la obtención de la situación actual de un entorno de información e informático en aspectos de seguridad y riesgo, eficiencia y veracidad e integridad.
- Las acepciones anteriores desde un punto de vista interno y externo.
- Auditoría como función de control dentro de un departamento de sistemas.

4.7.1.4. NORMAS DE T.I.

Entenderemos por normas de auditoría a los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de dicho trabajo para el presente trabajo que desempeña y a la información que rinde como resultado de dicho trabajo, para el presente trabajo clasificaremos en tres rubros a las normas de auditoría conforme lo define El Consejo Mexicano para la investigación y desarrollo de Normas de Información Financiera (CINIF) y la Federación Internacional de Contadores (IFAC), dichas normas se clasifican en.

1) Normas Personales, estas normas son referentes a lo relacionado con la formación del auditor y se dividen en tres grandes grupos:

    - Entrenamiento técnico y la capacidad profesional
    - Cuidado y diligencia profesional
    - Independencia

2) Normas de Ejecución del trabajo, esta división es referente a la ejecución de la función y a las actividades realizadas.

    - Planeación y supervisión
    - Estudio y evaluación del control interno
    - Obtención de evidencia suficiente y competente.

3) Normas de Información, esta división contiene todos los lineamientos referentes a los papeles de trabajo o legajos, así como los del resumen del resultado final, por lo que se debe contemplar lo siguiente.

    - Se debe de emitir un reporte escrito y firmado cada vez que se concluya con un examen de auditoria
    - Los auditores deberán discutir sus conclusiones y recomendaciones a un nivel adecuado de la administración antes de emitir su reporte escrito final.
    - Los reportes deberán ser objetivos claros, concisos, constructivos y oportunos, así mismo contendrán el propósito alcance y resultados de la auditoría y en lo aplicable, la opinión del auditor y además pueden incluir recomendaciones para mejorar así como el reconocimiento de la ejecución de acciones correctivas.
    - Pueden ser incluidos en el reporte de auditoría los puntos de vista de los responsables de las áreas auditadas, respecto de las conclusiones o recomendaciones del auditor.
    - El responsable de la función de auditoría deberá revisar y aprobar el reporte final de la auditoría antes de su emisión y decidirá a quién o quienes les será distribuido el reporte.

4.7.2. FUNCIONES DE LA AUDITORÍA EN T.I.

Hoy en día, con la evolución del uso y creación de las telecomunicaciones y de la tecnología, ha propiciado que las comunicaciones, líneas y redes de las instalaciones informáticas, así como el software y el hardware, los procesos de sistema operativo y la seguridad de los sistemas, se auditen por separado aunque formen parte del entorno general de sistemas. Dentro de la Auditoría en T.I. existen puntos críticos e indispensables a realizar, lo cual se describen en los siguientes apartados, la estructura, las funciones y características importantes que contiene ésta.

La misión de la función en auditoría en T.I., "es proveer a los órganos de gobierno ya los de gestión de una organización", es decir, debe de proveer una seguridad razonable de que los sistemas de control interno de los recursos de información de dicha organización estén bien definidos y efectivamente administrados, para apoyar y ayudar a la creación del valor de una organización.

Por lo anterior es importante que se tome en cuenta la definición del control interno, el cual es definido por informe COSO (Committee of Sponsoring Organization) en su primera versión como: "Un proceso ejercido por el consejo de administración de la entidad, los gestores y otro persona de la organización, diseñado para proporcionar seguridad razonable respecto a la consecución de los objetivos y dividido en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de la información financiera
- Cumplimiento con leyes y regulaciones

Se tiene en cuenta que los órganos de gobierno ecuatoriano en este sentido son los responsables de la gestión o dirección de la organización de las diferentes unidades de negocio o soporte que existen dentro de la organización que estos mismos son responsables de plasmar las metas, objetivos y las políticas, delimitaremos la responsabilidad de plasmar dichas actividades al comité de dirección bajo la responsabilidad de un director general.

Las actividades principales se enumeran a continuación:

1.- Verificación del control interno, tanto de las aplicaciones como de los sistemas de tecnología de información central y periféricos.

2.- Análisis de la gestión de los sistemas de información desde un punto de vista de riesgo de seguridad de gestión y efectividad de la misma.

3.- Análisis de la integridad, flexibilidad y certeza de la información a través del análisis de las aplicaciones.

4.- Auditoría del riesgo operativo de los circuitos de información.

5.- Análisis de la gestión de los riesgos de la información y de la seguridad implícita

6.- Verificación del nivel de continuidad de las operaciones

7.- Análisis de estado tecnológico de la instalación revisada y de las consecuencias empresariales que pudiesen darse dentro de la organización.

8.- Diagnóstico sobre el grado de cobertura que dan las aplicaciones a las necesidades estratégicas y operativas de información en la organización.

A este respecto definiremos como auditor al individuo o persona encargada de evaluar la eficiencia y eficacia de los sistemas de información dentro de una organización. El auditor tiene la virtud de oír y revisar, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y la eficacia con que está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan. El auditor de T.I. es encargado de la verificación y certificación de la información dentro de las organizaciones.

Es necesario que el personal que desempeña la función de auditoría en tecnología de información dentro de la organización debe cumplir con ciertos requisitos, tanto técnicos como administrativos, por lo que el auditor debe ser una persona con un alto grado de calificación técnica y al mismo tiempo estar integrado en las corrientes organizativas empresariales que imperan hoy en día, por ende se deben de contemplar las siguientes características dentro de su formación, se tiene en cuenta que debe ser una mezcla de conocimientos básicos de auditoría financiera y de auditoría general, contemplando los siguientes aspectos:

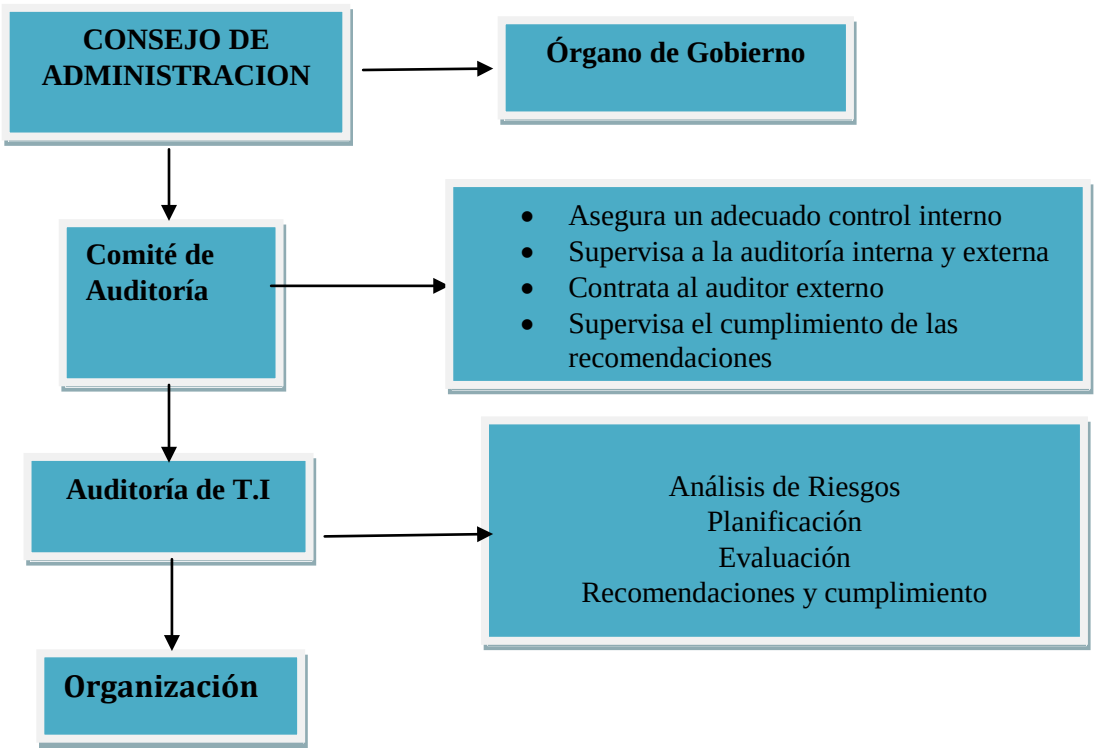
- Desarrollo informático; gestión de proyectos y del ciclo de vida de un proyecto de desarrollo
- Gestión del departamento de Sistemas
- Análisis de riesgo de un entorno informático.
- Sistema operativo (dependiendo de varios factores, pero como factor principal si se va a trabajar como auditor interno os si se desarrollará como auditor externo).
- Telecomunicaciones
- Gestión de bases de datos
- Redes locales
- Seguridad física
- Operaciones y planificación informática, efectividad de las operaciones y del rendimiento de los sistemas.
- Gestión de la seguridad de los sistemas y de la continuidad empresarial a través de planes de contingencia de la información
- Gestión de problemas y de cambios de entornos informáticos
- Administración de datos
- Comercio electrónico
- Encriptación de datos
- Conocimiento de técnicas, herramientas y generales en administración de negocios[62]

4.7.2.1. ESTRUCTURA DEL ÁREA DE AUDITORÍA EN T.I.

La ubicación de la función de auditoría en T.I. deberá estar englobada con la función de auditoría interna de dicha organización. En la actualidad existen normativas nacionales e Internacionales, así como buenas prácticas de gobierno corporativo, que establecen o recomiendan la posición y el rol que debe de tener la función de la auditoría interna en una organización. **(véase Ilustración No.35)**

[62] www.isaca.org, ISACA 2010

ILUSTRACIÓN 35 **ESTRUCTURA DEL ÁREA DE AUDITORIA DE TI**



Por lo antes mencionado la organización tipo de la auditoría en T.I., debe contemplar los siguientes principios:

1.- La localización la cual debe de estar ligada a la localización de la auditoría interna operativa y financiera, pero debe de tener independencia de objetivos, de planes de formación y de presupuestos.

2.- La organización operativa tipo debe ser la de un equipo independiente del de auditoría interna con la accesibilidad total a los sistemas de información e informáticos y dependerán de la misma persona en la empresa, que en cuyo caso deberá ser el director general.

Es importante mencionar que en caso de que exista una dependencia ésta será del máximo responsable operativo de la organización nunca del departamento de organización o del sistema, ni del departamento financiero y-o administrativo.

El departamento por otro lado deberá contemplar una mezcla equilibrada entre sus personas con formación en auditoría y gestión de la organización y personas con perfil en tecnología de información, sin embargo este perfil debe ser tratado con un amplio programa de formación en el cual se debe explicar no solo los objetivos de la función, sino también de la persona. Este personal

debe contemplar entre su titulación la de CISA[63]como un elemento básico. La organización en la función de auditoría en tecnología deberá cubrir los principales roles que a continuación se describen:

- Jefe del Departamento: Desarrolla el plan operativo del departamento, las descripciones de los puestos de trabajo del personal del cargo, las planificaciones de actuación a corto plazo y largo plazo, los métodos de gestión del cambio en su función y los programas de formación individualizados, así como gestionar los programas de trabajo y los trabajos en sí.
- Gerente o supervisor de auditoría en tecnología: Se encargará de evaluar los riesgos de cada uno de los trabajos, realizar los programas de trabajo, dirige y supervisa directamente a las personas en cada una de las tareas delegadas.
- Auditor en tecnología: Son responsables de la ejecución directa del trabajo, deben tener una especialización genérica, así como una específica, su trabajo consiste en la obtención de información, realización de pruebas, documentación del trabajo y diagnóstico de resultados.

[63] Certified Information Systems, certificado otorgado por ISACA

CAPÍTULO V.- MODELO DE DEMING

El modelo de Deming es un ciclo de mejoramiento continuo, es un proceso que describe muy bien lo que es la esencia de la calidad y refleja lo que las empresas necesitan hacer si quieren ser competitivas.

Una de las principales herramientas para la mejora continua en las empresas es el ya conocido por todos Ciclo Deming o también nombrado ciclo PHVA (planear, hacer, verificar y actuar). En realidad el ciclo fue desarrollado por Walter Stewart, el cual dio origen al concepto. Sin embargo los japoneses fueron los encargados de darlo a conocer al mundo, nombrándolo así en honor al Dr. William Edwards Deming, estadístico americano, lo asocian con el ascenso del Japón como nación industrial, y a la invención del Total Quality Management (Gestión de calidad total) TQM, enseñó muchos métodos de mejoramiento de la calidad a los japoneses, incluyendo el uso de la estadística y del ciclo PHVA.

El ciclo Deming es una secuencia lógica de cuatro pasos repetidos que se deben de llevar a cabo consecutivamente. Estos pasos son: Planear, Hacer, Verificar y Actuar.

En la presente tesis se explica cada uno de estos pasos, las técnicas y los beneficios de su aplicación; identificando en cada etapa algunas actividades a llevar a cabo, como: establecer los objetivos de mejora, aplicar soluciones y documentar acciones, vigilar los cambios que se hayan realizado y realizar los ajustes necesarios y/o aplicar nuevas mejoras en la administración de riesgos de TI, como marco de referencia se utiliza Cobit.

El mejoramiento continuo es una incesante búsqueda de problemas y sus soluciones. Por lo cual debemos de considerar el concepto fundamental del ciclo que es que nunca termina. Es un medio eficaz para desarrollar cambios positivos que van a permitir ahorrar dinero tanto para la empresa como para los clientes.

La alternativa de continuar con otro ciclo de mejoramiento, después de dejar el proceso bajo control, si no ahora, más adelante, requiere una buena documentación del proyecto actual, el análisis, la validación, las decisiones que se tomaron, los logros y lo que falta por mejorar..[64]

5.1.- IMPORTANCIA Y LOS PASOS A SEGUIR DENTRO DE LA UTILIZACIÓN DEL MODELO DE DEMING

La gestión de calidad Deming es un sistema de medios para generar económicamente productos y servicios que satisfagan los requerimientos del cliente. La implementación de este sistema necesita de la cooperación de todo el personal de la organización, desde el nivel gerencial hasta el operativo e involucramiento de todas las áreas.

Según la óptica de este autor, (Eduardo Deming), la administración de la calidad total requiere de un proceso constante, que será llamado Mejoramiento Continuo, donde la perfección nunca se logra pero siempre se busca.

[64] El método Deming en la práctica / Mary Walton, W. Edwards Deming, Bogotá, Traducción Margarita Cárdenas - Grupo Editorial Norma - Bogotá, 2004.

El Mejoramiento Continuo es un proceso que describe muy bien lo que es la esencia de la calidad y refleja lo que las empresas necesitan hacer si quieren ser competitivas a lo largo del tiempo.

Los pasos que sugiere Deming para lograr éxitos en la búsqueda de calidad son los siguientes:

Crear constancia en el propósito para la mejora de productos y servicios.

El Dr. Deming sugiere una nueva definición radical del papel que desempeña una compañía. En vez de hacer dinero, debe permanecer en el negocio y proporcionar empleo por medio de la innovación, la investigación, el constante mejoramiento y el mantenimiento.

La gerencia tiene dos clases de problemas, dice el Dr. Deming: los de hoy y los de mañana. Los problemas de hoy tienen que ver con las necesidades inmediatas de la compañía: como mantener la calidad, el presupuesto; el empleo; las utilidades; el servicio; las relaciones públicas
.
Ninguna compañía que carezca de un plan para el futuro, podrá continuar en el negocio. Los empleados que trabajan para una compañía que está invirtiendo para el futuro, se sienten más seguros y están menos deseosos de buscar otro empleo.

Habrá que tener una declaración de constancia en el propósito que significa:

1.- Innovación.- Consiste en la introducción de algún producto, por el solo hecho de tener algo nuevo que vender, debe tener algún beneficio. Todo plan debe responder a las siguientes preguntas satisfactoriamente.

¿Qué equipos se requerirán? ¿A qué costo? ¿Cuál será el método de obtención de información? ¿Qué gente nueva deberá contratarse? ¿Qué cambios serán necesarios en el equipo? ¿Qué nuevas habilidades se requerirán, y para cuánta gente? ¿Cómo serán entrenados en estas nuevas capacidades los empleados actuales? ¿Cómo serán capacitados los supervisores? ¿Cuál será el costo de capacitación e innovación tecnológica? ¿Cuál será el costo de mercadeo? ¿Cuáles serán el costo y el método de servicio? ¿Cómo sabrá la compañía si el cliente está satisfecho?

2.- Investigación e instrucción.- Con el fin de prepararse a futuro, una compañía debe invertir hoy. No puede haber innovación sin investigación, y no puede haber investigación sin empleados apropiadamente instruidos.

3.- Mejoramiento continuo del sistema de administración de riesgos.- Esta obligación con el consumidor nunca termina. Se pueden obtener grandes beneficios mediante un continuo proceso de mejoramiento del diseño y del desempeño de productos ya existentes. Es posible, y realmente fácil, que una organización entre en decadencia si erróneamente se dedica a un sistema de administración de riesgos desactualizado, aunque todos los elementos de la compañía se desempeñen con dedicación y empleen los métodos estadísticos y todas las demás ayudas que puedan estimular la eficiencia.

4.- Mantenimiento de los equipos y sistemas de administración de riesgos.- Obviamente una compañía no puede mejorar su sistema de administración de riesgos de tecnología con equipos que no funcionan bien ni pueden detectar riesgos inherentes al negocio. Es necesario invertir en estas áreas.

5.- Adoptar una nueva filosofía.- La calidad debe convertirse en la nueva religión. Hay nuevos estándares. Ya no podemos darnos el lujo de vivir con errores, defectos, mala calidad, malos

materiales, manejando daños, trabajadores temerosos e ignorantes, entrenamiento deficiente o nulo, cambios continuos de un empleo a otro por parte de los ejecutivos y un servicio desatento y hosco.
Las empresas rara vez aprenden de la insatisfacción de sus clientes. Los clientes no se quejan, simplemente cambian de proveedor. Sería mejor tener clientes que elogien el producto.

6.- Dejar de confiar en la inspección masiva.- Las firmas norteamericanas inspeccionan un sistema de manera característica cuando sale de la línea de creación o en etapas importantes. Los sistemas defectuosos, o bien se desechan, o bien se reprocesan; tanto lo uno como lo otro es innecesariamente costoso.
La inspección que se hizo con el ánimo de descubrir los procesos ineficaces ya es demasiado tardía, ineficaz y costosa. La calidad no se produce por la inspección, sino por el mejoramiento del proceso.

Como cuestión práctica, siempre será necesario ejercer cierto grado de inspección, aunque sea para averiguarlo que se está haciendo. En algunos casos, podría ser necesaria una inspección del 100%, por razones de seguridad.

La inspección debe de llevarse a cabo de manera profesional, no con métodos superficiales, el objetivo de toda compañía de ser abolir la calidad por inspección. La inspección no debe dejarse para el sistema final, cuando resulta difícil determinar en qué parte del proceso se produjo un defecto.

7.- Poner fin a la práctica de conceder negocios con base en el precio únicamente.- Los departamentos de compras tienen la costumbre de actuar sobre los pedidos en busca del proveedor que ofrezca el precio más bajo. Con frecuencia, esto conduce a suministros de baja calidad.

Tiene tres serias desventajas: la primera es que, casi invariablemente, conduce a una proliferación de proveedores. La segunda es que ello hace que los compradores salten de proveedor en proveedor. Y la tercera es que se produce una dependencia de las especificaciones, las cuales se convierten en barreras que impiden el mejoramiento continuo.

La mejor forma de servirle un comprador a su compañía es desarrollando una relación a largo plazo de lealtad y confianza con un solo proveedor, en colaboración con el departamento de ingeniería y de otros departamentos, para reducir los costos y mejorar la calidad.

8.- Mejorar constantemente y por siempre el sistema de administración de riesgos de tecnología.- El mejoramiento no se logra de buenas a primeras. La gerencia está obligada a buscar continuamente maneras de reducir el desperdicio de tiempo, esfuerzos y dinero en procesos inoperantes y de mejorar la calidad.

Hay que incorporar la calidad durante la etapa del diseño, y el trabajo en equipo es esencial para el proceso.

Una vez que los planes están en marcha, los cambios son costosos y causan demoras. Todo el mundo y todos los departamentos de la compañía deben convenir en implantar el mejoramiento continuo. Este no debe limitare a los sistemas de producción o de servicio. Los de compras, transporte, ingeniería, mantenimiento, ventas, personal, capacitación y contabilidad, todos tienen un papel que desempeñar.

La gerencia debe tomar la iniciativa. Solamente la gerencia puede iniciar el mejoramiento de la calidad y la productividad. Es muy poco lo que los trabajadores empleados en la producción pueden lograr por si solos. La eliminación de un problema irritante o la solución de un problema particular, no forma parte del mejoramiento de un proceso.

Mediante el uso de datos interpretados apropiadamente pueden tomarse decisiones inteligentes.

9.- Instituir la capacitación.- Con mucha frecuencia los trabajadores han aprendido sus labores de otro trabajador que nunca fue entrenado apropiadamente. Se ven obligados a seguir instrucciones imposibles de entender. No pueden desempeñar su trabajo porque nadie les dice cómo hacerlo.

Es muy difícil borrar la capacitación inadecuada, esto solamente es posible si el método nuevo es totalmente diferente o si a la persona la están capacitando en una clase distinta de habilidades para un trabajo diferente.

Por otra parte, la capacitación no debe finalizar mientras el desempeño no haya alcanzado el control estadístico y mientras haya una posibilidad de progreso. Todos los empleados tendrán que recibir alguna capacitación en el significado de la variación, y es preciso que tenga un conocimiento rudimentario de los gráficos de control.

10.- Instituir el liderazgo.- El trabajo de un supervisor no es decirle a la gente qué hacer o castigarla, sino, orientarla. Orientar es ayudarle a la gente a hacer mejor el trabajo y conocer por medio de métodos objetivos quién requiere ayuda individual.

Ejercer el liderazgo es tarea de la gerencia. Es responsabilidad de la gerencia descubrir las barreras que les impiden a los trabajadores enorgullecerse de lo que están haciendo. En lugar de ayudar a los trabajadores a hacer su trabajo en forma correcta, la mayor parte del personal de supervisión hace exactamente lo contrario.

En la actualidad, frecuentemente el trabajo es tan nuevo para el supervisor como para los trabajadores, se sienten cómodos en un sistema que les impone a los empleados cantidad o cuotas.

La tarea del gerente es guiar, ayudarles a los empleados a realizar mejor su trabajo. Al contratarlos, la gerencia asume la responsabilidad de su éxito o fracaso.

La mayor parte de las personas que no realizan bien su trabajo no son holgazanes que fingen estar enfermos para no trabajar, sino que simplemente han sido mal ubicadas. Si alguien tiene una incapacidad o no puede realizar un trabajo, el gerente tiene la obligación de encontrar un lugar para esa persona.

11.- Eliminar el temor.- Muchos empleados temen hacer preguntas o asumir una posición, aun cuando no entiendan en que consiste el trabajo, o qué está bien o que está mal.

Las personas que ocupan posiciones gerenciales, no entienden en que consiste su trabajo ni lo que está bien o mal, no saben cómo averiguarlo. Muchas temen hacer preguntas o asumir una posición.

La gente tiene miedo de señalar los problemas por temor de que se inicie una discusión o que lo culpen del problema.

La gente teme perder su aumento de sueldo o su ascenso, o lo que es peor su empleo. Teme que le asignen trabajos punitivos o que le apliquen otras formas de discriminación. Temen que sus

superiores puedan sentirse amenazados y se desquiten de algún modo si se muestra demasiado audaz. Teme por el futuro de su compañía y por la seguridad de su empleo. Teme admitir que cometió errores.

Para lograr mejor calidad y productividad, es preciso que la gente se sienta segura. Los trabajadores no deberán tener miedo de informar sobre un equipo dañado, de pedir instrucciones o de llamar la atención sobre las condiciones que son perjudiciales para la calidad.

12.- Derribar las barreras que hay entre las áreas.- Con frecuencia, las áreas de staff, departamentos o secciones, están compitiendo entre sí o tienen metas que chocan entre sí.

Esto sucede cuando los departamentos persiguen objetivos diferentes y no trabajan en equipo para solucionar los problemas, para fijar las políticas o para trazar nuevos rumbos.

Aunque las personas trabajen sumamente bien en sus respectivos departamentos, si sus metas están en conflictos, pueden arruinar a la compañía. Es mejor trabajar en equipo, trabajar para la compañía.

13.- Eliminar los lemas, las exhortaciones y las metas de producción para la fuerza laboral.-

Estos nunca le sirvieron a nadie para hacer un buen trabajo. Los eslóganes generan frustraciones y resentimientos. Una meta sin un método para alcanzarla es inútil. Pero fijar metas sin describir como han de lograrse es una práctica común que debe de eliminarse. Es totalmente imposible para cualquier persona o para cualquier grupo desempeñarse fuera de un sistema estable, cualquier cosa puede suceder.

La tarea de la gerencia, tal como hemos visto, es tratar de estabilizar los sistemas. Un sistema inestable produce una mala impresión de la gerencia.

14.- Eliminar las cuotas numéricas.- Las cuotas sólo toman en cuenta los números, no la calidad o los métodos. Por lo general, constituyen una garantía de ineficiencia y de altos costos.

Las cuotas u otros estándares de trabajo tales como el trabajo diario calculado, obstruyen la calidad más que cualquier otra condición de trabajo. Los estándares de trabajo garantizan la ineficiencia y el alto costo.

A menudo incluyen tolerancia para artículos defectuosos y para desechos, lo cual es una garantía de que la gerencia los obtendrá.

En ocasiones la gerencia fija expresamente un estándar de trabajo por lo alto, con el propósito de descartar a la gente que no puede cumplirlo. Cuando las cuotas se fijan para los que pueden cumplirlas, la desmoralización aun es mayor.

Los incentivos estimulan a la gente para que produzcan cantidad en vez de calidad. Incluyen los costos de trabajo rechazado, repetido o de menor calidad como elementos de la ecuación. En algunos casos, los trabajadores son objetos de deducciones salariales por razón de las unidades defectuosas que producen.

Un estándar de trabajo apropiado definirá lo que es y lo que no es aceptable en cuanto a calidad. La calidad aumentará a una tasa cada vez mayor de esa etapa en adelante. En lugar de asignarle cuotas a un trabajo, se debe estudiar dicho trabajo y definir los límites de dicho trabajo.

15.- Remover las barreras que impiden el orgullo por un trabajo bien hecho.- La gente está ansiosa por hacer un buen trabajo, y se siente angustiada cuando no puede hacerlo.

A medida que mejora la calidad, también mejora la productividad. A menudo los gerentes se conmocionan cuando se enteran de lo que anda mal. Los trabajadores se quejan de que no saben de un día para otro lo que de ellos se esperan. Los estándares cambian con frecuencia. Los supervisores son arbitrarios. Rara vez se les proporciona una retroalimentación de su trabajo hasta que conozcan las evaluaciones del desempeño o se hagan aumentos de sueldo, y entonces ya será demasiado tarde.

Hoy en día, a la gente la consideran como si fuera una mercancía que se usa cuando se necesita. Si no se necesita, se devuelve al mercado.

Una cortina de humo es un medio al que recurre el gerente para aparentar que está haciendo algo al respecto de un problema. Tales programas muestran una notable tendencia a desvanecerse, porque la gerencia nunca les confiere autoridad alguna a los empleados ni actúa sobre sus decisiones o recomendaciones. Los empleados se decepcionan más aún.[65]

16.- Instituir un programa vigoroso de educación y recapacitación.- Tanto la gerencia como la fuerza laboral tendrán que ser entrenadas en el empleo de los nuevos métodos.

El hecho de que usted tenga gente buena en su organización no es suficiente. Ella debe estar adquiriendo continuamente los nuevos conocimientos y las nuevas habilidades que se necesitan para manejar nuevos materiales y nuevos métodos. La educación y el reentrenamiento son necesarios para la planificación a largo plazo.

A medida que mejora la productividad, se requerirá menos gente en algunos casos. Quizá se agreguen algunos puestos, pero otros pueden desaparecer. Debe poner en claro que nadie perderá su empleo debido al aumento en la productividad.

La educación y el entrenamiento deben preparar a la gente para asumir nuevos cargos y responsabilidades.

Habrá necesidad de una mayor preparación en estadística, en mantenimiento y en la forma de tratar con los proveedores. La preparación en técnicas estadísticas, sencillas pero poderosas, será necesaria en todos los niveles.

17.- Tomar medidas para llevar a cabo la transformación.- Se requerirá un equipo de altos ejecutivos con un plan de acción para llevar a cabo la misión que busca la calidad. Los trabajadores no están en condiciones de hacerlo por su propia cuenta.

Todos los empleados de la compañía, incluyendo los gerentes, deben tener una idea precisa de cómo mejorar continuamente la calidad. La iniciativa debe venir de la gerencia. El ciclo Deming hoy en día constituye el elemento esencial del proceso de planificación.

Paso 1: el primer paso es estudiar un proceso, decidir qué cambio podría mejorarlo.
Paso 2: efectúe las pruebas, o haga el cambio, preferentemente en pequeña escala.
Paso 3: observe los efectos.

[65] http://www.elprisma.com/apuntes/administracion_de_empresas/aplicacioncalidadtotal/default5.asp

Paso 4: ¿que aprendimos? .Para lograr la transformación es vital que todos empiecen a pensar que el trabajo de cada cual, debe proporcionarles satisfacción a un cliente.

5.2.- ESQUEMA DE IMPLANTACIÓN DEL SISTEMA DE CALIDAD DEMING

En base a las siguientes variables definitorias se establece el esquema de implantación del sistema de calidad que contribuyen a mantenerse como empresa del mercado de valores con resultados altamente rentables en: rendimiento, clientes, personal y sociedad. Las variables son: Misión, Enfoque, Esquema Estructural, Sistema de Retroalimentación, Criterios y Subcriterios, y por último los conceptos o principios fundamentales.

Misión: El Modelo Gerencial Deming tiene como misión crear un sistema organizativo que fomente la cooperación, tanto interna como externa así como un aprendizaje que facilite la implementación de prácticas de gestión de procesos. Esto lleva a una mejora continua de procesos, productos y servicios, así como de satisfacción del trabajador, fundamentalmente para la satisfacción del cliente y para la supervivencia de la organización. Método dirigido a quienes apuestan y arriesgan por la empresa, es decir, un método que defina los resultados para los clientes, empleados, sociedad y todos aquellos que poseen un riesgo financiero en la organización.

Enfoque.- El modelo basa su enfoque en el control estadístico, en la resolución de problemas y en perfeccionamiento o mejora continua.

Esquema Estructural.- A partir de las relaciones dinámicas e integradas entre los criterios. A un nivel básico, si un proceso es clave o crucial para la organización dentro de los "Agentes o Procesos facilitadores" y los restantes a la categoría de los "Resultados". **(Véase Ilustración No.36)**

ILUSTRACIÓN 36 ESQUEMA ESTRUCTURAL DEL SISTEMA DE CALIDAD DEL CICLO DE DEMING

AGENTES FACILITADORES	RESULTADOS
1.- Liderazgo y estilo de dirección	En los clientes
2.- Personas	En las personas
3.- Política y estrategia	En la Sociedad
4.- Alianzas y recursos	Claves y globales
5.- Procesos	

5.3. BALANCED SCORECARD O CICLO DE ADMINISTRACIÓN DEL PDCA (PLAN, DO, CHECK AND ACT) EN EL MERCADO DE VALORES ECUATORIANO

A partir de un punto de vista general del mercado de valores ecuatoriano, el concepto de ciclo de administración, es ¨una serie de actividades que planifican y controlan el trabajo diario con el fin de alcanzar los objetivos de la manera más eficiente y efectiva manteniendo un equilibrio entre cantidad y Costo.

Antes de realizar el análisis es importante señalar que lo primordial es un pensamiento estratégico de la organización, esto es que la supervivencia empresarial radica no en tanto en la calidad de la planeación a largo plazo, sino en la claridad del pensamiento estratégico. P-Drucker. La planificación a largo plazo no es pensar en decisiones futuras sino en el futuro de las decisiones presentes. Los imperativos gerenciales deben ser:

- Alinear a la empresa con su estrategia
- Obtener resultados concretos de sus activos intangibles
- Pasar del control financiero al control estratégico
- Administrar basados en la estrategia

5.3.1.- ¿QUÉ ES ESTRATEGIA?

La estrategia es un marco de referencia que orienta y limita aquellas decisiones que determinan la naturaleza y dirección de la organización. Consiste en diferenciarse de la competencia porque la empresa es única en algo que es valioso para sus clientes.

Tener una estrategia es importante, pero lo es más aún la habilidad para ejecutar esa estrategia y solo se logra cuándo toda la organización esté alineada y enlazada con la estrategia.

Los competidores pueden fácilmente copiar las mejoras de calidad y eficiencia, pero no pueden copiar su posicionamiento estratégico, lo que distingue a la empresa del resto.

La estrategia intenta alcanzar una ventaja competitiva sostenible preservando lo que es distinto en la empresa. La estrategia es la creación de una única y valiosa posición involucrando un conjunto de actividades que la empresa requiere hacer.

La estrategia competitiva son las acciones ofensivas o defensivas de la empresa para crear una posición defendible dentro del mercado de valores. Acciones que son la respuesta a las cinco fuerzas competitivas determinantes de la naturaleza y el grado de competencia que rodea a una empresa y que como resultado, busca obtener un importante rendimiento sobre la inversión. La efectividad operacional significa realizar estas actividades mejor- esto es, más rápido o con menos entradas y defectos-que los rivales.

Barreras para implementar la estrategia

1.- Solo el 5% de la fuerza laboral entiende la estrategia de la empresa

2.- Solo el 25% de los empleados tienen incentivos ligados a la Estrategia

3.- 60% de las Organizaciones no tienen ligados los presupuestos a la Estrategia

4.- 85% de los ejecutivos invierte no más de una hora al mes en discutir la Estrategia

5.- Porque los objetivos individuales de quienes la tienen que aplicar no están alineados

6.- Porque no hay un balance entre los objetivos a largo plazo y los de corto plazo

7.- Porque no se identifican indicadores de desvíos o aciertos (control de gestión)

8.- Porque no se identifican los procesos críticos para alcanzar la estrategia

9.- Porque no se desarrollan las competencias del personal responsable de su ejecución

La empresa debe definir dos necesidades: 1.- Definir la estrategia 2.- Implementarla. Definir la misma puede resultar complicado pero en la implementación es donde la mayoría encuentra la mayor dificultad.

¿Cómo crear valor para la empresa?

La estrategia se basa en una diferenciada propuesta de valor a los clientes, lo cual se crea en los procesos internos de la organización. Desarrollar esa estrategia implica considerar una serie de temas complementarios y simultáneos que están relacionados con los activos intangibles de la organización, pero solo el alineamiento estratégico determina el valor de los activos intangibles, siendo precisamente éstos los que crean ventaja competitiva.

El valor de la empresa dentro del mercado de valores tiene dos componentes definidos: Sus activos físicos o financieros(Inventarios, cuentas por cobrar, titularización de cartera, edificio y Maquinaria) y los activos no financieros compuestos por tres capitales: Capital Humano que representa el activo más valioso de una organización siempre y cuando esté alineado con la estrategia, posea las competencias, habilidades, destrezas y conocimiento necesario para el logro de la nueva estrategia organizacional.

Por si solo no brinda ningún valor, convirtiéndose más bien en un costo. El capital de la información se basa en las bases de datos, redes y tecnología necesaria para el uso del recurso humano que brinde la mejora continua de los procesos y por último el Capital Organizacional está relacionado con la cultura o clima organizacional el cual depende en gran medida del estilo del liderazgo, la forma en que se desarrolle el trabajo en equipo y de cómo estén alineados los sistemas de reconocimiento con la estrategia.

5.3.2.- ¿QUÉ ES EL BSC (BALANCED SCORECARD O CUADRO DE MANDO INTEGRAL)?

Es un conjunto coherente de elementos que conectan acciones con la estrategia, es un sistema de ayuda a la planificación y gestión que facilita la comunicación y proporciona mejor información a todos los niveles.

Centrado en el contenido. El software es un medio no un fin en sí mismo.

Enfocado en los objetivos estratégicos y las iniciativas prioritarias. Los cambios en la evaluación y en la compensación son una consecuencia y no la razón de ser del modelo.

El BSC es más que un nuevo sistema de medición, es el marco y estructura central de los procesos organizacionales, el poder del BSC aparece cuando se transforma de un sistema de indicadores en un sistema de gestión.

La corriente gerencial de la organización en estudio considera al BSC como sistema de mejora continua o Círculo de Deming conocido por sus siglas en inglés como el PDCA.

5.3.2.1.- PLANIFICAR (PLAN)

Al establecer un Sistema de Gestión de Riesgos de Seguridad de la Información, se debe implantar la política de seguridad, objetivos, metas, procesos y procedimientos relevantes para manejar riesgos y mejorar la seguridad de la información para generar resultados de acuerdo con una política y objetivos marco de la organización. Es importante instituir objetivos de corto y largo plazo, sus estrategias, indicadores e iniciativas desde las cuatro perspectivas necesarias para alcanzar la visión definida de la empresa. **(Véase Ilustración No.37)**

- Identificar los temas estratégicos, establecimiento del contexto en el que se desarrolla la empresa dentro del mercado de valores.
- Plantear las hipótesis en una correlación causa efecto
- Desarrollar el Mapa Estratégico
- Construir la Matriz del Cuadro de Mando
- Desplegar la estrategia a los siguientes niveles
- Valoración de los riesgos, en este caso esquemático a presentar sería dentro de un proceso en lo particular.
- Desarrollo de tratamiento de riesgos
- Aceptación de los riesgos

Se debe definir el alcance del SGRS a la luz de la organización.- Ser consistentes en los objetivos

ILUSTRACIÓN 37 ANÁLISIS DE RIESGOS (PLAN)

Analizando esta gráfica se debe de:

- Identificar y evaluar opciones para tratar los riesgos identificados: Mitigar, Eliminar, Transferir y Aceptar, dentro del alcance definido.
- Seleccionar los objetivos de control y controles a implementar (Mitigar), en virtud del resultado del análisis de riesgos, considerando a su vez los requisitos legales y regulatorios que rigen al mercado de valores ecuatoriano. Y a partir de los 133 controles definidos por la ISO-IEC-27005
- Establecer enunciado de aplicabilidad.- Selección o no de cada uno de los controles y explicación. **(véase Ilustración No.38)**

ILUSTRACIÓN 38 CUADRO DE LOS CONTROLES ISO-IEC-27005

Edición 2005		Objetivos	Controles
5	Política de Seguridad	1	2
6	Aspectos organizativos para la seguridad	2	11
7	Gestión de los activos	2	5
8	Seguridad de los Recursos Humanos	3	9
9	Seguridad física y del entorno	2	13
10	Gestión de comunicaciones y operaciones	10	32
11	Control de accesos	7	25
12	Adquisición, Desarrollo y mantenimiento de sistemas	6	16
13	Gestión de incidentes de seguridad de la información.	2	5
14	Gestión de continuidad del negocio	1	5
15	Conformidad	3	10
Totales		39	133

5.3.2.2.-IMPLEMENTAR Y OPERAR (DO)

Implementar y operar el Sistema de Gestión de Riesgos de Seguridad de la Información mediante controles, procesos y procedimientos.

Implementar el plan de tratamiento de riesgos: Transferir, Eliminar, Aceptar, Mitigar, esto es clave para el éxito de la implementación.

Implementar programas de capacitación y concientización continua.

Implementar procedimientos y controles de detección y respuesta a incidentes, y por último

Implementar indicadores para medir la eficacia de los controles

5.3.2.3.-MONITOREO Y REVISIÓN (CHECK)

Evaluar y medir la performance de los procesos contra la política de seguridad, los objetivos y experiencia práctica y reportar los resultados a la dirección para su revisión.

Revisar el nivel de riesgo residual aceptable, considerando los cambios en el entorno, Auditorías internas son indispensables, revisiones por parte de la dirección.

5.3.2.4.-MANTENIMIENTO Y MEJORA (ACT)

Tomar acciones correctivas y preventivas basadas en los resultados de la revisión de la dirección para lograr la mejora continua del Sistema de Gestión de Riesgos.

Identificar mejoras en el SGR a fin de implementarlas

Tomar las acciones apropiadas (preventivas y correctivas)

Comunicar los resultados y las acciones a emprender y consultar con todas las partes involucradas

Revisar el SGR donde sea necesario implementando las acciones seleccionadas.

Precisamente la información se encuentra desarrollada con toda claridad en los capítulos anteriores de esta tesis.

5.4.- CATEGORÍAS, CLASIFICACIÓN Y CONDICIONES DE LAS ACTIVIDADES DE CONTROL DE ACUERDO AL DESARROLLO DEL CONTROL INTERNO.

5.4.1.- DEFINICIÓN DE CONTROL.

Para el mejor entendimiento de este texto se iniciará con el término de Control o también conocida como actividad de control.

Control o Actividad de control ¨Es cualquier medida que tome la dirección, el Consejo y otros, para mejorar la gestión de riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planifica organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas¨[66]

Los controles o actividades de control son medidas aplicables para todo el entorno de la empresa y generalmente se conocen como controles generales, pero dentro de estas actividades de control se encuentran aquellos que se han especificado y son aplicables a una sola área como es la tecnología de información.

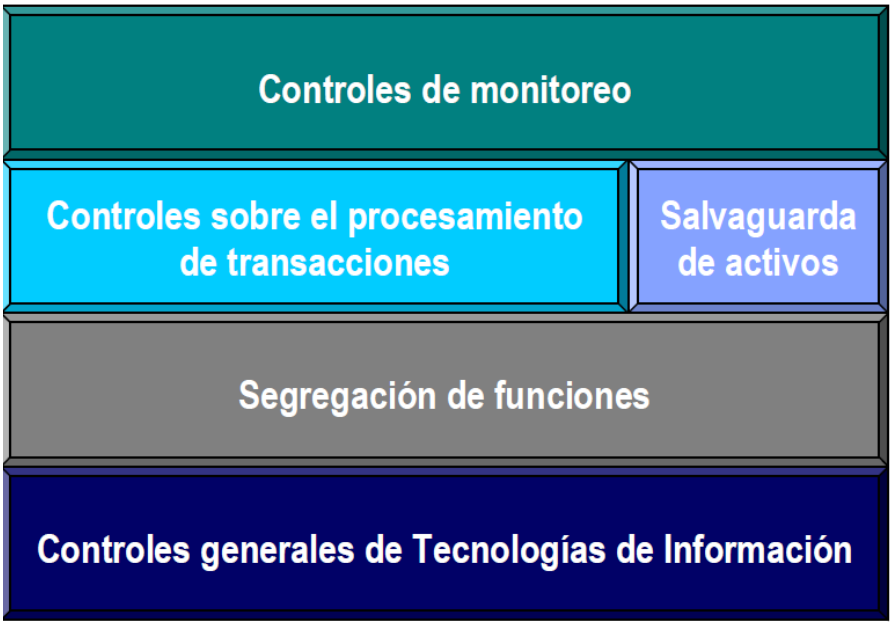
A continuación se mencionarán categorías, clasificaciones y condiciones con las que deben de cumplir los controles o actividades de control.

5.4.2.- CATEGORÍA DE LOS CONTROLES GENERALES DE ACUERDO A COSO.

Los controles son los medios diseñados para contrarrestar los riesgos identificados y pueden ser clasificados de acuerdo al Control Interno general y al marco referencial COSO en:

- **Controles de monitoreo.**- actividades de control que ayudan a la gerencia a validar de manera periódica las acciones que se ejecutan en determinado proceso del negocio tales como los márgenes, número de cuentas nuevas, número de facturas procesadas, etc. Para identificar errores originados por la falta o funcionamiento incorrecto de controles a nivel de transacciones, y monitorear el logro de las metas financieras y operacionales.
- **Controles a nivel de transacciones.**- actividades de control dirigidas a asegurar que los datos (órdenes, facturas, cobranza, etc.), estén completos, sean válidos y exactos, y para cumplir con los objetivos de control establecidos para diferentes procesos.
- **Controles de salvaguarda de activos.-**actividades de control referidos a la custodia de los activos e incluyen controles y medidas de seguridad diseñadas para asegurar que el acceso a los activos e incluyen controles y medidas de seguridad diseñadas para asegurar que el acceso a los activos se limite sólo al personal autorizado, como son: bienes muebles e inmuebles, efectivo o documentos al cobro y registro de datos.
- **Controles de segregación de funciones.-** actividades de control diseñadas para prevenir que una persona esté en posición de controlar distintas etapas del procesamiento de una transacción son que otra persona detecte errores o irregularidades, si los mismos se producen.
- **Controles Generales de Tecnologías de Información.-** actividades de control que ayudan a asegurar el acceso a programas y datos (Seguridad física y lógica), comprobar operaciones computacionales, verificar mantenimiento y cambio de programas y revisar el desarrollo de programación (PWC, 2006). **(véase Ilustración No.39)**

ILUSTRACIÓN 39 CONTROLES O ACTIVIDADES DE CONTROL



Con la anterior clasificación, se puede captar en que parte de acuerdo al COSO se ubican los controles generales de Tecnologías de Información. Conforme a esta imagen, se puede ver que son los controles que sirven de base para los demás debido a su naturaleza de soporte, ya que las Tecnologías de Información, son las que contiene la gran mayoría de la información operacional de la empresa a través de sus sistemas de información, redes, bases de datos, servidores, equipos de cómputo, etc. De ahí radica la importancia de que se requiera proteger estos bienes.

5.4.3.- CLASIFICACIÓN DE LOS CONTROLES

Ahora bien, lo controles generales y controles de TI en su contexto general, pueden tener las siguientes clasificaciones de acuerdo a su naturaleza de origen y a la forma en que se lleva a cabo. Estos controles son aplicables a cualquier tipo de control en cualquier nivel de la organización.

Los controles se dividen en:

a.- Acorde a su aplicación sobre el riesgo: Preventivos y Detectivos

b.- Acorde a la forma en que se llevan a cabo en: Automáticos y Manuales

a.- Preventivos y Detectivos

- Preventivos.- Están diseñados para evitar el procesamiento de transacciones con errores o irregularidades, identificándolas y rechazándolas antes de completar el procesamiento.

  Ejemplo: contar con un formato de alta de usuarios para el acceso a las aplicaciones, debidamente autorizado por la gerencia de la cual proviene. Previniendo así que las altas de usuarios se realicen sin permiso.

- Detectivos.- Están diseñados para identificar errores o irregularidades una vez ocurrido el proceso.
  Ejemplo: Realizar un monitoreo remoto de instalaciones de software en equipos de usuario. Este control detecta que software es instalado sin autorización.

b.- Automáticos y Manuales

- Automáticos.- Son aquellos soportados por los sistemas de aplicación e involucra una comparación, efectuada por el sistema de determinada información relativa a una transacción con una serie de parámetros pre-establecidos.

  Ejemplo: la aplicación verifica que el nombre de usuario y contraseña son válidos para acceder al mismo. Cuando se realicen verificaciones del funcionamiento de estos controles, se recomienda que sólo se prueben una vez, ya que la aplicación si está programada correctamente siempre funcionará bien, de lo contrario siempre habrá errores.

- Manuales.- Son aquellos llevados a cabo por los funcionarios de la organización y su efectividad está sujeta a la responsabilidad, capacidad, experiencia del funcionario que los realiza y la segregación de funciones.

  Ejemplo: Para realizar una modificación aun programa o sistema se requiere de una solicitud formal de cambio por parte del dueño de la información hacia el área de

desarrollo, debido a que los desarrolladores no deben realizar alteraciones a las aplicaciones sin el consentimiento del dueño.

5.4.4.- CONDICIONES PARA LOS CONTROLES

Las circunstancias con las que deben disponer los controles para proporcionar una seguridad razonable son expuestas a continuación:

- **Proporcionar efectividad y eficiencia en las operaciones.**- A causa de que el uso de controles disminuye el riesgo, por consecuencia los procesos son más efectivos y eficientes. Este es uno de los objetivos de negocio básicos de una entidad, incluyendo las metas de desempeño y de rentabilidad. Esto incluye la protección de los activos, tangibles e intangibles.
- **Suministrar confiabilidad de los reportes financieros.-** En la aplicación de controles, podemos asegurarnos que la información sea completa, exacta y válida, viéndose reflejado en reportes arrojados por las aplicaciones. Y a su vez en la preparación confiable de reportes financieros, presentados de manera razonable y en conformidad con principios de contabilidad generalmente aceptados (GAAP) u otros principios apropiados diferentes a GAAP.
- **Cumplir con leyes y regulaciones aplicables.-** Incluye cumplimiento con las reglas de la SEC (Securities and Exchange Commission) reglas del mercado de valores y reglas de pago de impuestos sobre utilidades, las cuales tienen un impacto financiero.

5.5.- CONTROL INTERNO

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimento de leyes y reglamentos.

Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

No todas las personas entienden lo mismo por Control Interno, esto se agrava cuando sin estar claramente definido se utiliza en la normatividad.

En sentido amplio, se define como: un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objetivo de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Confiabilidad de la información financiera

- Cumplimiento de las leyes y normas aplicables.

La anterior definición refleja ciertos conceptos fundamentales:

- El control interno es un proceso, un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El control interno lo llevan a cabo las personas, no se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.
- El control interno sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la Dirección y al Consejo de Administración de la Entidad.
- El control interno está pensado para facilitar la consecución de objetivos propios de cada entidad.[67]

5.5.1.- COMPONENTES DEL CONTROL INTERNO

El control interno consta de cinco componentes relacionados entre sí, se derivan de la manera en que la dirección dirige la empresa y están integrados en el proceso de dirección, los componentes del control son:

1.- El ambiente de Control

2.- La Evaluación de Riesgos

3.- Los Sistemas de Información y Comunicación

4.- Los procedimientos o actividades de control

5.- Supervisión o vigilancia

Los cuales se detallan a continuación:

1.- **Ambiente de Control**

El ambiente de control se sirve de base para todos los otros componentes de la gestión de riesgos, proporcionando la disciplina y la estructura.

El ambiente de control influye en la estrategia y en los objetivos establecidos, estructurando las actividades del negocio, identificando, evaluando e interpretando los riesgos. Es decir, que el ambiente de control incide sobre el funcionamiento de las actividades de control, la información, los sistemas de comunicación y las actividades de supervisión.

Como parte del ambiente de control, la dirección establece filosofía de gestión de riesgos, determinando el grado de riesgo que asumirá la organización. Se entiende como grado de riesgo que la organización está dispuesta a aceptar para el logro de su objetivo.

[67] PWC, 2006, Pricewaterhouse Coopers (Ed), ¨Manual de Curso GO SPA 2006¨,México

2.- Evaluación de riesgos

La evaluación de riesgos permite a la organización considerar los potenciales acontecimientos que pudieran afectar el logro de los objetivos. La probabilidad representa la posibilidad que un acontecimiento ocurra, mientras que el impacto representa su efecto.

La metodología de evaluación de riesgos de una organización normalmente comprende una combinación de técnicas cualitativas y cuantitativas. En aquellos casos donde los riesgos no son cuantificables, o cuando no se poseen datos suficientes y creíbles para evaluaciones cuantitativas, a menudo se utilizan solo técnicas de evaluación cualitativa, sin embargo, no se debe olvidar que la cuantificación brinda mayor precisión en la evaluación de riesgos.

Al momento de evaluar los acontecimientos no se debe realizar individualmente, sino que s se debe tener en cuenta la correlación que pudiera existir entre distintos acontecimientos y las secuencias de acontecimientos y las secuencias de acontecimientos que se combinan e interactúan para crear los impactos sobre la organización.

3.- Sistemas de Información y comunicación

La información, tanto interna como externa debe ser identificada, captada y comunicada en tiempo y forma para poder así evaluar los riesgos y establecer la respuesta a los mismos.

Dado que la información se origina en diversas fuentes (internas, externas) y tiene diferentes características (cualitativa, cuantitativa), se genera un gran desafío que es el de contar con un gran volumen de información, del que deberá ser captada la información relevante, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores, permitiendo asumir las responsabilidades individuales.

4.- Actividades de control

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que la respuesta a los riesgos, sea correctamente efectuada. Las actividades de control ocurren en todos los niveles y funciones de la organización.

5.- Supervisión o vigilancia

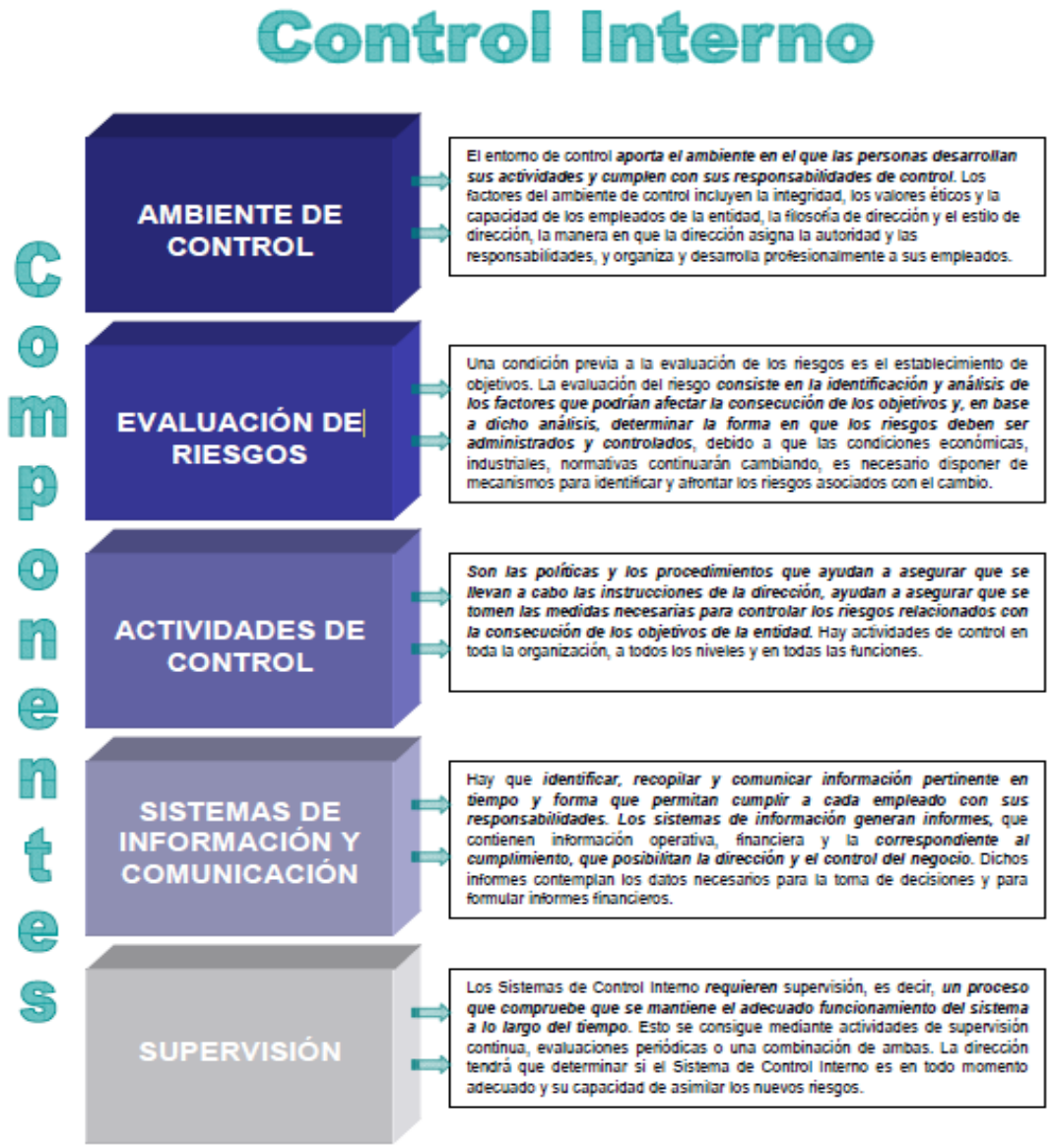
La gestión de riesgos debe ser supervisado y tal supervisión puede hacerse en tiempo real o posterior, siendo la primera forma la más eficaz.

Una vez que tenemos un enfoque acerca de lo que es el control interno, podemos retomar que es una actividad que comúnmente se lleva a cabo en la empresa, y que a través de la implementación, desarrollo y cumplimiento de objetivos se efectúa. Este puede estar inherente, es decir, que se encuentra ahí por naturaleza, simplemente porque existe algún tipo de control dentro de la empresa: o puede estar de manera formal, en el cual se puede encontrar ampliamente documentado mediante políticas, procedimientos, manuales, descripciones, entre otras formas de documentación.

El control interno es aplicable para todos los niveles y área de la organización, ya que en todas estas áreas se realizan actividades y procesos recurrentes, quienes ejecutan para cumplir con metas y objetivos, los cuales son monitoreados para evaluar su nivel de desempeño, basándose en políticas y planes en los cuales deben existir dueños de cada actividad y proceso quienes sean responsables de la ejecución de estos mismos.

Algunas áreas donde se efectúa el control interno son: Compras, Ventas, Capital Humano, Almacén, Inventarios, Tecnologías de Información. Etc. Este último jugando un papel muy importante en la actualidad, ya que soportan gran parte de la información que se maneja dentro de la empresa [68](COSO, 2008). **(Véase Ilustración No.40)**

ILUSTRACIÓN 40 MAPA MENTAL DE CONTROL INTERNO



[68] COSO, 2008

CAPÍTULO VI.- CASO ESQUEMÁTICO DE UNA ADMINISTRACIÓN DE RIESGOS ASOCIADOS A LAS T.I. EN UN PROCESO DE NEGOCIO ESPECÍFICO DE UNA EMPRESA PARTICIPANTE EN EL MERCADO DE VALORES

Se pretende realizar un análisis de riesgos de seguridad de la información que permita a la organización del mercado de valores ecuatoriano en forma general, dado a que se presenta limitaciones en la obtención de la información real por ser considerado información altamente confidencial tanto en las instituciones de mi país como las de México. Los objetivos son:

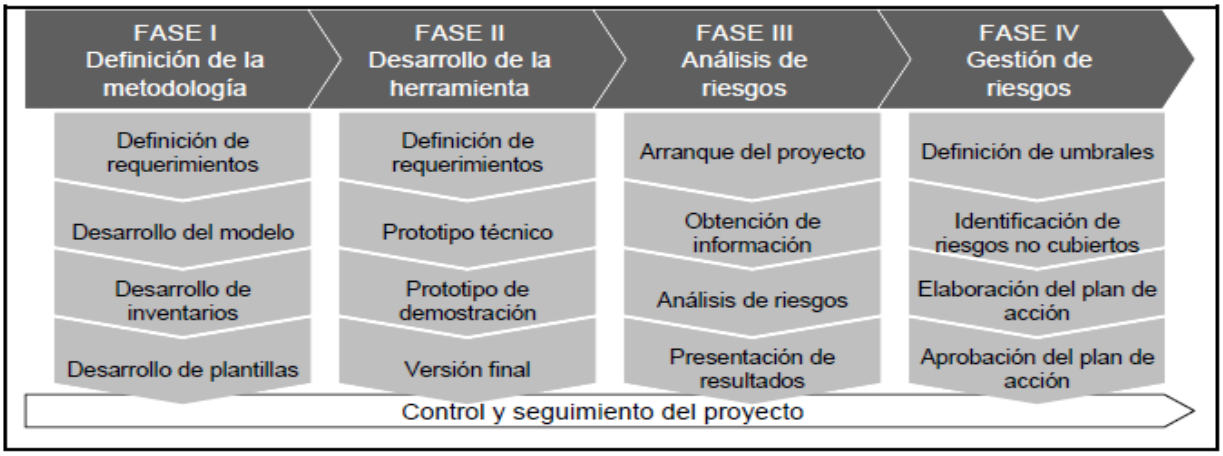
- Definir formalmente los requerimientos de seguridad de la información en función de sus necesidades y con ello dimensionar adecuadamente la inversión y la estructura necesaria para soportar la Seguridad de la Información [ISO27001.05] [ISO27001.05].
- Desarrollar una metodología de análisis de riesgos de seguridad de Información formal basado en estándares internacionales, que conjugue la compatibilidad con las metodologías existentes en la actualidad con las necesidades de la Organización en la materia. [ISO27005.08] [NIST800/18.98].
- Desarrollar una herramienta que facilite la realización del análisis de riesgos y su posterior mantenimiento.

El modelo especifica que el análisis de riesgos debe considerarse un ciclo por el que, tras la gestión del riesgo se sitúa una nueva iteración del análisis de riesgos que permite obtener la evolución de los procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas y de esta forma reajustar permanentemente el nivel de riesgo a los requerimientos de la Organización.

6.1.-FASES DEL PROYECTO

El desarrollo de este proyecto se ha organizado en cuatro fases que se describen en el siguiente gráfico junto con las principales actividades de cada una: **(véase Ilustración No.41)**

ILUSTRACIÓN 41 FASES DEL PROYECTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE TI



El objetivo de cada una de las fases se describe a continuación:

FASE I: Definición de la metodología

Definición de la metodología a emplear durante el proyecto, partiendo de las metodologías estándar de análisis de riesgos, combinándolas y adaptándolas a los requerimientos específicos de la Organización.

FASE II.- Desarrollo de la herramienta

Desarrollo de una herramienta que soporte la realización de análisis de riesgos utilizando la metodología desarrollada.

FASE III: Análisis de riesgos

Empleo de la metodología y la herramienta para la realización de un análisis de riesgos que soporte la implantación de un SGSI (Sistema de Gestión de la Seguridad de la Información) en la Organización.

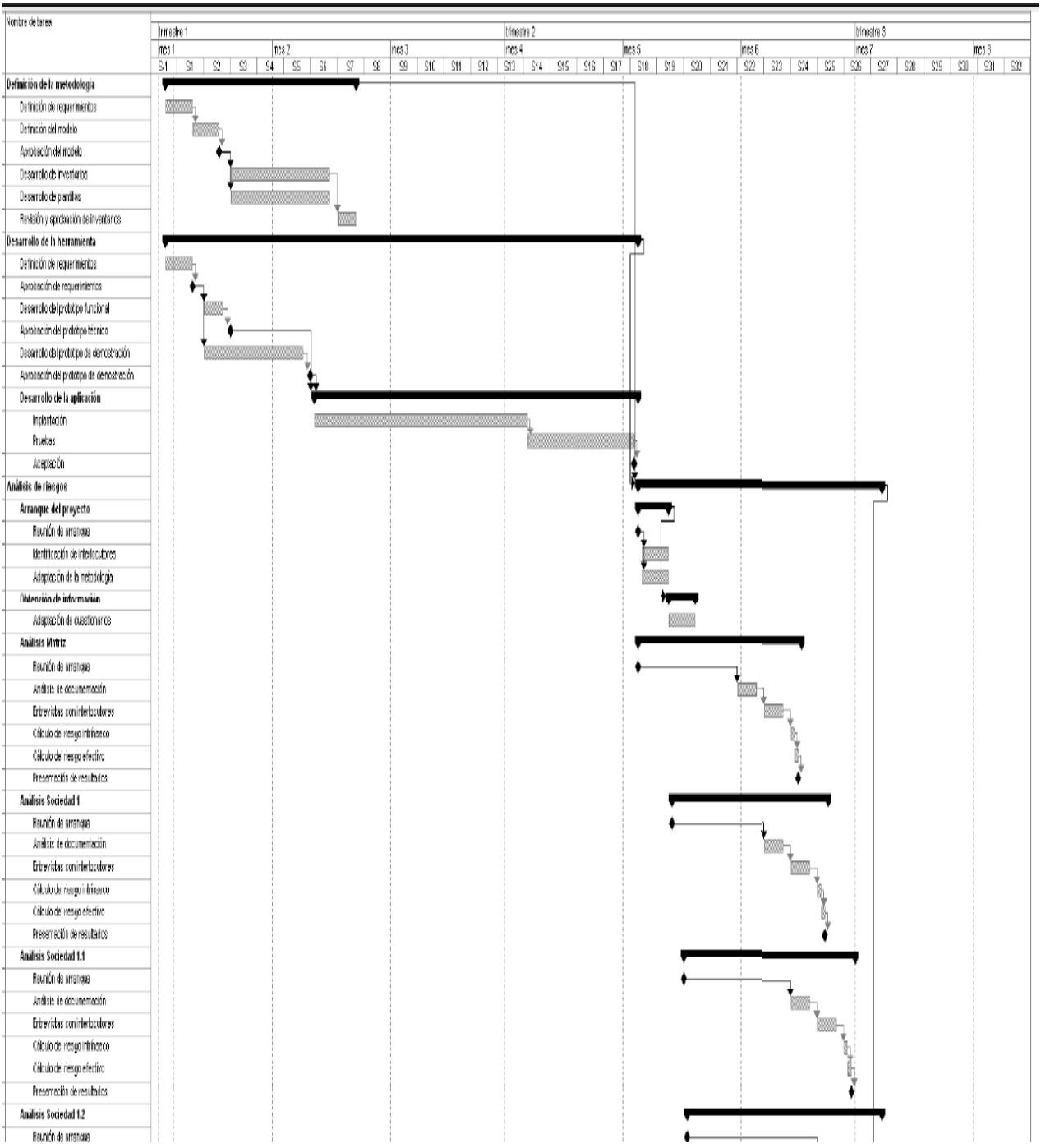
FASE IV: Gestión de riesgos

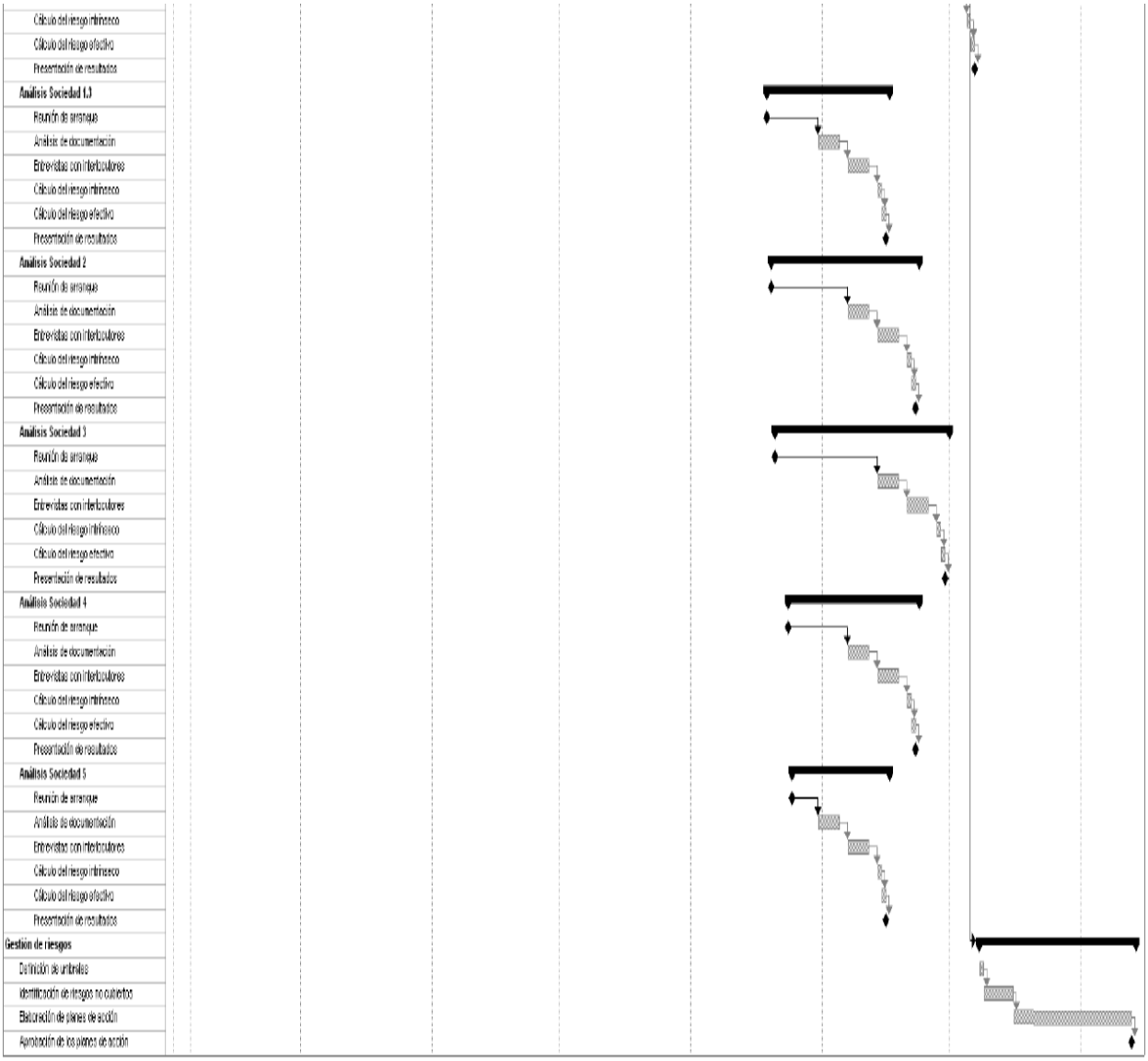
Desarrollo de un plan de acción en base a la estrategia de gestión de riesgos definida por la organización y los resultados del análisis de riesgos realizado

En los siguientes apartados se puede encontrar una descripción más detallada de las tareas realizadas correspondientes a cada fase y actividad. **(Véase Ilustración No.42)**

La planificación general del proyecto queda resumida en el siguiente diagrama Gantt:

ILUSTRACIÓN 42 DIAGRAMA DE GANTT, PLANIFICACIÓN DEL PROYECTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE TI

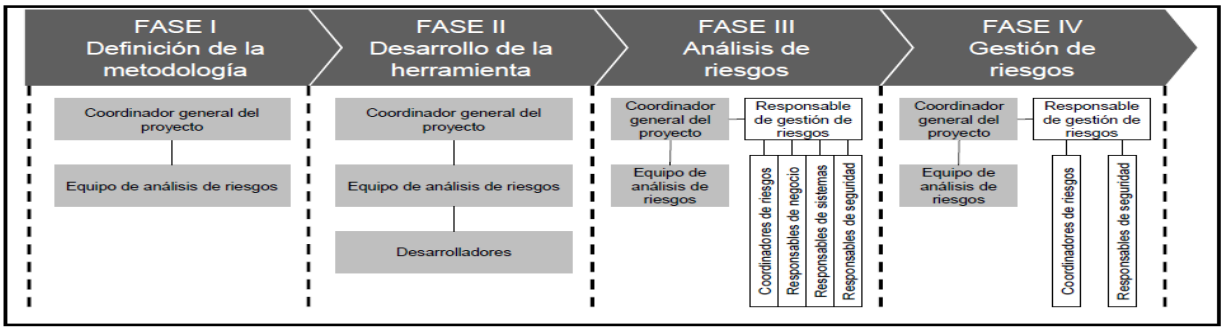




Equipo de trabajo

El equipo de trabajo definido para la ejecución de cada una de las fases del proyecto fue el siguiente. (Asignación de responsabilidades detallada en el capítulo 4): **(Véase Ilustración No.43)**

ILUSTRACIÓN 43 ORGANIZACIÓN DEL EQUIPO DE TRABAJO



6.1.1.-FASE I DEFINICIÓN DE LA METODOLOGÍA

Definición de requerimientos.- Teniendo en cuentas las distintas metodologías disponibles para hacer el análisis de riesgos, se decidió desarrollar una metodología adaptada específicamente a las necesidades de la Organización.

Las características deseables en la metodología a desarrollar son los siguientes:

- Basada en estándares, para aprovechar conocimiento y herramientas que permitan la realización de comparaciones con otras organizaciones
- Sencillez y facilidad de uso, tanto en el momento de la primera implantación como el mantenimiento.
- Enfocada a los procesos de negocio y de soporte de la Organización
- Modular y adaptable que pueda adaptarse a diferentes entornos
- Objetiva, los resultados no deben depender de quién aplique la metodología ni de cómo lo haga

Dada las características deseables para la metodología, se han desarrollado unos principios para su desarrollo:

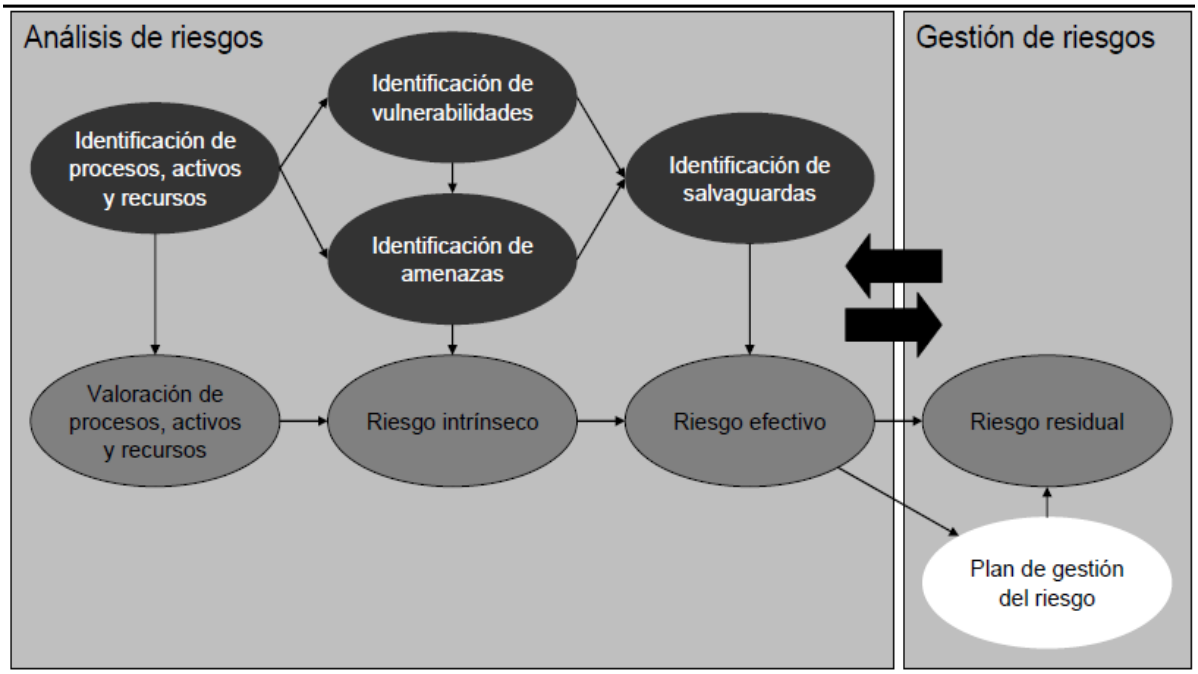
- Metodología mixta con entrada de datos cualitativa, para facilitar la comunicación entre las distintas partes que deben participar en el análisis y métodos de cálculo cuantitativos para aprovechar la mayor eficiencia computacional y mayor precisión en los resultados.
- Utilización de los principios básicos comunes a las principales metodologías de análisis de riesgos estándar. Utilización de principios, estándares y metodologías estándar en los aspectos que se deban tratar y no cubran las metodologías estándar de análisis de riesgos
- Eliminación de los elementos que aporten menor valor o no son considerados de un nivel considerable de afectación al negocio ni en la consecución de los objetivos, en aras de mayor facilidad de uso y claridad.

- Que disponga de diversos inventarios de tipos de activos, amenazas y salvaguardas, de modo que se pueda utilizar con sencillez y que se pueda adaptar fácilmente a distintas necesidades y objetivos del análisis.
- Que disponga de una herramienta de soporte específica que facilite la entrada de datos y la realización de los cálculos.
- Que disponga de todos los elementos habituales que permiten dotar de objetividad al proceso: acuerdo entre varios expertos, objetivos de valoración y proporcionar ejemplos con valores de referencia reales.

6.1.1.1- DESARROLLO DEL MODELO

Modelo de la metodología.- Para definir la presente metodología se ha considerado el modelo que forma la base de todas las metodologías estándar de análisis de riesgos, y se han seleccionado las diferentes alternativas disponibles para la definición del modelo teniendo en cuenta los principios descritos en los capítulos 3 y 4 de la presente tesis. **(Véase Ilustración No.44)**

ILUSTRACIÓN 44 MODELO GENERAL DE LA METODOLOGÍA DE ANÁLISIS DE RIESGOS



En primer lugar, el modelo diferencia dos fases:

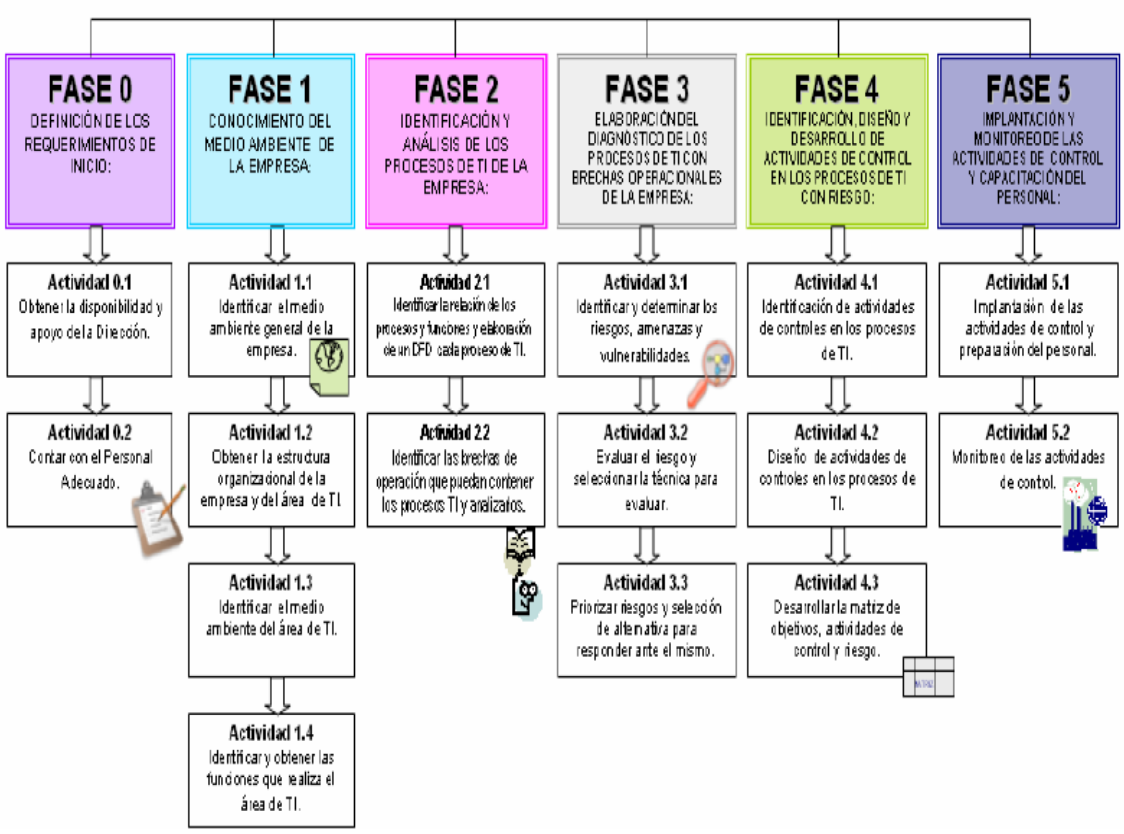
- Análisis de riesgos, que compre la obtención de información referente a procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas.
- Gestión de riesgos, que comprende la definición de la estrategia a seguir para ajustar el nivel de riesgo a los requerimientos de la Organización.

En este modelo se distinguen por colores tres tipos de elementos:

- Inventario de activos, vulnerabilidades, amenazas y salvaguardas.
- Valoración de activos, vulnerabilidades, amenazas y salvaguardas para la obtención del riesgo intrínseco, efectivo y residual.
- Plan de gestión del riesgo.

Por último, el modelo especifica que el análisis de riesgos debe considerarse un ciclo por el que, tras la gestión del riesgo se sitúa una nueva iteración del análisis de riesgos que permite obtener la evolución de los procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas y de esta forma reajustar permanentemente el nivel de riesgo a los requerimientos de la Organización. **(Véase Ilustración No.45)**

ILUSTRACIÓN 45 MATRIZ ESQUEMÁTICA DE LA METODOLOGÍA A DESARROLLAR



6.2.- CATEGORÍA Y ESTRUCTURA DE LOS RIESGOS

Para poder estructurar una clara categoría de los riesgos es indispensable tener claro los **criterios de evaluación de los riesgos** dentro del mercado de valores los principales son:

1.- Valor estratégico del proceso de negocio

2.- Criticidad de los activos de información dentro del proceso analizado

3.- Leyes, regulaciones y contratos

4.- Confidencialidad, Integridad y Disponibilidad

5.- Expectativas, percepciones y daño a la reputación

Criterios de Impacto

1.- Clasificación del activo impactado

2.- Violaciones de la seguridad (C, I, D)

3.- Operaciones afectadas (internas o a terceros)

4.- Pérdida de negocio y valor financiero

5.- Violaciones a leyes, regulaciones o contratos

6.- Interrupción a los planes y fechas límites

Criterios de aceptación de riesgos

1.- Criterios del negocio

2.- Aspectos legales y regulatorios

3.- Operaciones

4.- Tecnología

5.- Finanzas

6.- Factores sociales y humanos

Es importante **diferenciar l**os factores que componen a los riesgos: Activo, Vulnerabilidad, Amenaza o Impacto.

Dentro de una correcta ejecución de un análisis de riesgos de seguridad de la información los pasos que se aplicará en este caso práctico son como resultado de un estudio exhaustivo, claro, preciso y sencillo.

Establecimiento del contexto.- Hemos ya establecido el contexto para la gestión de riesgos de seguridad de la información del mercado de valores a lo largo de los cinco capítulos de esta tesis. La primera parte está totalmente analizada.

A continuación para poder establecer e identificar los riesgos se debe seleccionar un proceso de negocio en este caso el que vamos a escoger es el principal proceso que administra el mercado de valores, la titularización de la cartera.

6.2.1.- ANÁLISIS DEL PROCESO DE TITULARIZACIÓN DE CARTERA

La titularización engloba el proceso a través del cual la cartera crediticia o los activos financieros se transforman en títulos valores. La titularización tiene como objetivo canalizar el ahorro eliminando la intermediación financiera e incentivando la movilización de cartera.

Es una herramienta financiera a través de la cual se transfiere parte de los activos de una empresa a un patrimonio autónomo que se encarga de emitir títulos respaldados en los flujos futuros de dichos activos con la finalidad de obtener recursos. El proceso de la titularización se da inicio a través de la conformación de un patrimonio autónomo mediante la transferencia de la Cartera de Crédito Comercial (C.C.C.), el cual servirá de garantía para establecer un contrato con una fiduciaria, éste a su vez será el encargado de emitir instrumentos de deuda para colocarlos a los inversionistas o mercado de valores.

El dinero que se obtiene producto de la venta de los títulos fluye de los inversionistas a la Sociedad Administradora de los fondos y de ésta hacia el originador.

Se pueden titularizar los activos que existen o que se espera que existan, que conlleven la expectativa de generar flujos futuros determinables, sea de fondos o sea de derechos de contenido económico. No puede pesar sobre dichos activos ninguna clase de gravámenes, limitaciones al dominio, prohibiciones de enajenar, condiciones suspensivas o resolutorias, ni debe estar pendiente de pago de impuestos, tasas o contribuciones.

Son activos susceptibles de titularización:

a. Valores representativos de deuda pública
b. Valores inscritos en el Registro del Mercado de Valores
c. Cartera de crédito
d. Activos y proyectos inmobiliarios
e. Activos o proyectos susceptibles de generar flujos futuros determinables.

6.2.1.1.- ACTIVIDADES A SEGUIR EN UN PROCESO DE TITULARIZACIÓN DE CARTERA

1. Tomar la decisión de iniciar el proceso de titularización de un activo que conformara “el patrimonio autónomo” para la obtención de recursos.
2. Contactar a un estructurador con el fin de recibir asesoría en lo concerniente a los aspectos legales y financieros que conlleva dicho proceso con el objetivo de fijar las características

de la titularización, tales como: garantía, valor nominal, número de títulos, plazo, monto y rendimiento de la emisión.

3. Analizar las características propuestas por el estructurador en base a los riesgos inherentes en los flujos de tal manera que el originador pueda aceptar o rechazar dichas características.
4. Contratar a una Administradora de Fondos y Fideicomisos que se encargará de armar el fideicomiso mercantil.
5. Recopilar documentos e información para la aprobación del proceso por parte de la Superintendencia de Compañías.
6. Contratar a una calificadora de riesgos y a una Casa de Valores para que se encarguen de calificar el riesgo de la emisión y buscar a los posibles inversionistas, respectivamente. Además se deberá contratar una Compañía de Auditoria Externa por el tiempo que dure la emisión.
7. Proporcionar toda la información necesaria a la Superintendencia de Compañías para que autorice la oferta pública de valores.
8. Presentar la oferta pública a las Bolsas de Valores para su aprobación y negociación.
9. Establecer la fecha a partir de la cual se negociaran los valores en el mercado.
10. Vender todos los valores producto de la titularización.

6.2.- IDENTIFICAR LOS RIESGOS

La identificación de los riesgos de seguridad de la información, en el proceso de titularización de cartera y específicamente dentro de las actividades que se realizan, para lograrlo es necesario identificar:

- Activos
- Amenazas
- Controles existentes
- Vulnerabilidades
- Consecuencias/Impactos

Y la posibilidad de que todo esto pueda ocurrir en un mismo momento. La forma de realizarlo depende del enfoque del análisis de riesgos.

La identificación de activos de información de la organización debe realizarse a un nivel de detalle apropiado. También se deben identificar los dueños de los activos y los procesos de negocio a los que pertenecen. El estándar ISO/IEC 27005-2008 distingue los siguientes tipos de activos:

Primarios.- Procesos y actividades del negocio (información)

Activos de soporte.- Hardware, Software, Red, Personal, Sitio, Estructura organizacional.

Los dividiremos en 8 categorías: Ambiente, Procesos, Empoderamiento. Tecnologías de información. Integridad, Precio, Liquidez, Crédito. (ANEXO 1)

6.2.1.-OBTENCIÓN DE INFORMACIÓN

Antes de comenzar el proceso de la herramienta de análisis de riesgo se deben de preparar cuestionarios que permitan la toma de datos más eficaz, eficiente y homogénea. En la elaboración de los cuestionarios se tuvo en cuenta tanto las necesidades de información de la metodología como las adaptaciones particulares para el proceso de titularización de cartera de la empresa del mercado de valores.

Se prepararon los siguientes cinco cuestionarios: (Anexo 5)

1.- Preguntas para obtener la información acerca de la organización del personal

2.- Preguntas que se deberá realizar para obtener la información acerca de los sistemas

3.- Preguntas para descubrir los problemas de TI

4.- Preguntas para averiguar la Gestión de Riesgos de Seguridad de Tecnologías de Información

5.- Preguntas de autoevaluación de Gobierno de TI con relación a la Administración de Riesgos de Seguridad de la Información (Anexo 5)

6.2.1.1.- ENTREVISTAS CON INTERLOCUTORES O DUEÑOS DE PROCESOS

El contenido de las entrevistas mantenidas con los diferentes intervinientes de las diferentes áreas fue el siguiente:

- Breve presentación del proyecto de análisis de riesgos al interlocutor, para asegurar que conoce el contexto en el que se solicita su colaboración y para poder responder cualquier duda.
- Análisis de los procesos de negocio y de soporte por el interlocutor, revisando sus clasificaciones como relevantes o no relevantes de cara al análisis de riesgos. La principal información a obtener fue:
    - Objetivos del proceso
    - Subprocesos, tareas y actividades principales del proceso
    - Identificar quién asume las principales funciones y responsabilidades del proceso, teniendo en cuenta la Matriz RACI:
      R……...……. Realiza
      A……...Responsable
      C……Colabora
      I……..….Informa
- Identificación y valoración de los activos de información relevantes del proceso de titularización de cartera en este caso específico incluido dentro del alcance del análisis, tomando como punto de partida la información preparada por el equipo de análisis de riesgos con la documentación recibida y el cuestionario cumplimentado previamente por el interlocutor. La principal información a recabar de los activos de información es:

    - Nombre y descripción del activo de información

- Uso del activo de información en el contexto de la ejecución del proceso.
- Valoración de los requerimientos de seguridad del activo de información.

- Identificar las vulnerabilidades que puedan ser explotadas por las amenazas identificadas y que causen daño al activo en estudio.

- Identificar las amenazas y las consecuencias en la pérdida de confidencialidad, integridad y disponibilidad que pudiera tener en los activos seleccionados.

6.2.2.- IDENTIFICAR LOS ACTIVOS

En este caso práctico se enlistaran y clasificaran todos los activos más representativos que afectan a los procesos de negocio dentro del mercado de valores ecuatoriano. **(véase Ilustración No.46)**

ILUSTRACIÓN 46 LISTADO DE LOS ACTIVOS CONTEMPLADOS DENTRO DE UNA INSTITUCIÓN DEL MERCADO DE VALORES ECUATORIANO

Clase de Activo	**Entorno de TI global**	**Nombre del activo**	**Clasificación de activo**
	Máximo nivel de descripción del activo	**Definición de siguiente nivel (si es necesario)**	**Clasificación de valor de activo (1-5)**
Tangible	Infraestructura física	Centro de datos	5
Tangible	Infraestructura física	Servidores	3
Tangible	Infraestructura física	Equipos de escritorio	1
Tangible	Infraestructura física	Equipos móviles	3
Tangible	Infraestructura física	PDA	1
Tangible	Infraestructura física	Teléfonos móviles	1
Tangible	Infraestructura física	Software de aplicación de servidor	1
Tangible	Infraestructura física	Software de aplicación de usuario final	1
Tangible	Infraestructura física	Herramientas de desarrollo	3
Tangible	Infraestructura física	Enrutadores	3
Tangible	Infraestructura física	Conmutadores de red	3
Tangible	Infraestructura física	Equipos de fax	1
Tangible	Infraestructura física	PBX	3
Tangible	Infraestructura física	Medios extraíbles (por ejemplo, cintas, CD-ROM, DVD, Memory card, USB, discos duros portátiles, etc.)	1
Tangible	Infraestructura física	Fuentes de alimentación	3
Tangible	Infraestructura física	Sistemas de alimentación ininterrumpida	3
Tangible	Infraestructura física	Sistemas contra incendios	3
Tangible	Infraestructura física	Sistemas de aire acondicionado.	3
Tangible	Infraestructura física	Sistemas de filtrado de aire	1
Tangible	Infraestructura física	Otros sistemas de control ambiental	3
Tangible	Datos de intranet	Código fuente	5
Tangible	Datos de intranet	Datos recursos humanos	5
Tangible	Datos de intranet	Datos financieros	5
Tangible	Datos de intranet	Datos de publicidad	5
Tangible	Datos de intranet	Contraseñas de empleados	5
Tangible	Datos de Intranet	Claves de cifrado de sistema informático	5
Tangible	Datos de Intranet	Claves de cifrado privadas de empleado	5
Tangible	Datos de Intranet	Tarjetas inteligentes	5
Tangible	Datos de Intranet	Propiedad intelectual	5
Tangible	Datos de Intranet	Datos de requisitos normativos(Ley de protección da tos	5
Tangible	Datos de Intranet	Números de seguridad social	5
Tangible	Datos de Intranet	Planes estratégicos	3
Tangible	Datos de Intranet	Identificadores biométricos de los empleados	5
Tangible	Datos de Intranet	Datos de contacto personales de empleados	3
Tangible	Datos de Intranet	Datos de solicitudes de titularización de cartera	3
Tangible	Datos de Intranet	Datos de solicitudes de compra de bonos	3

Clase de Activo	Entorno de TI global	Nombre del activo	Clasificación de activo
	Máximo nivel de descripción del activo	**Definición de siguiente nivel (si es necesario)**	**Clasificación de valor de activo (1-5)**
Tangible	Datos de Intranet	Diseño de infraestructura de red	3
Tangible	Datos de Intranet	Sitio web internos	3
Tangible	Datos de Extranet	Datos financieros de socios	5
Tangible	Datos de Extranet	Datos de contratos con socios y clientes	5
Tangible	Datos de extranet	Clave de cifrado de socios	5
Tangible	Datos de extranet	Aplicación de colaboración con socios	3
Tangible	Datos de extranet	Claves de cifrado de socios y clientes	3
Tangible	Datos de extranet	Datos de contratos con proveedores	5
Tangible	Datos de extranet	Datos financieros de proveedores	5
Tangible	Datos de Internet	Aplicación de ventas de títulos de crédito en sitio web	3
Tangible	Datos de Internet	Datos de publicidad de sitio Web	5
Tangible	Datos de Internet	Datos de cotización de tasas de interés	5
Tangible	Datos de Internet	Claves de cifrado públicas	1
Tangible	Datos de Internet	Notas de prensa y noticias de servicios bursátiles	1
Tangible	Datos de Internet	Documentación de los servicios bursátiles	1
Intangible	Reputación		5
Intangible	Buena voluntad		5
Intangible	Moral de empleados		3
Intangible	Productividad del empleado		3
Servicios de TI	Sistemas Financieros	Ingreso de activos financieros (certificados de depósito a término, bonos, acciones, títulos hipotecarios, divisas, títulos de tesorería, aceptaciones bancarias, fondos de inversión, títulos de capitalización, pagaré, etc.)	5
Servicios de TI	Sistemas Financieros	Datos de ingreso y salida de usuarios acreditados	3
Servicios de TI	Mensajería	Correo electrónico	3
Servicios de TI	Mensajería	Mensajería Instantánea	1
Servicios de TI	Mensajería	Microsoft Outlook Web Access	1
Servicios de TI	Infraestructura básica	Microsoft Active Directory	3
Servicios de TI	Infraestructura básica	Sistema de nombres de dominio(DNS)	3
Servicios de TI	Infraestructura básica	Protocolo de configuración dinámica de host (DHCP)	3
Servicios de TI	Infraestructura básica	Herramientas de administración bursátil	3
Servicios de TI	Infraestructura básica	Uso compartido de archivos	3
Servicios de TI	Infraestructura básica	Almacenamiento de datos	3
Servicios de TI	Infraestructura básica	Acceso telefónico remoto	3
Servicios de TI	Infraestructura básica	Telefonía	3
Servicios de TI	Infraestructura básica	Acceso a red privada virtual(VPN)	3
Servicios de TI	Infraestructura básica	Servicio de nombres de Internet	1

Una vez identificados los activos de toda la empresa escogemos los más significativos que afectan al proceso de titularización de cartera y se elaborará un cuadro explicativo por las actividades dentro de este proceso. Cabe resaltar que para efectos de aplicación se escogerá siete activos a manera de ejemplo. **(Véase Ilustración No.47)**

ILUSTRACIÓN 47 CUADRO DE CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

ACTIVO	CLASIFICACIÓN	NIVEL DE VALOR DE IMPACTO AL PROCESO DE NEGOCIO
1.- Base de datos de activos financieros	Sistemas de Información Financiera	1
2.- Datos de ingreso y salida de usuarios o clientes	Sistemas de Información Financiera	1
3.- Red de comunicaciones	Infraestructura básica	3
4.- Servidores y Site de Computo	Infraestructura física	3
5.-Software de aplicación de servidor principal	Infraestructura física	1
6.- Personal operativo del sistema financiero	Intranet de RR.HH	5
7.- Sistemas de respaldo de información financiera	Infraestructura física	5

6.2.3.- IDENTIFICACIÓN DE VULNERABILIDADES

La presencia de una vulnerabilidad, por sí misma no es dañina, necesita existir una amenaza que la explote. Deben identificarse tanto las vulnerabilidades intrínsecas como extrínsecas al activo. Es decir pueden ser propias del activo o por otras situaciones como la falta o falla de un control o el uso inapropiado del activo. **(Véase Ilustración No.48)**

Proceso: Titularización de Cartera
Actividad: Ingreso de los aspectos legales y financieros
Activo: Base de datos de activos financieros

ILUSTRACIÓN 48 CUADRO DE VULNERABILIDADES Y NIVEL DE EXPLOTACIÓN

VULNERABILIDADES	Pueden ser explotadas por
1.- Fallas conocidas en el software	T1
2.- Falta de pistas de auditoría	T2
3.- Incorrecta asignación de privilegios de acceso	T3
4.- Falta de documentación	T4
5.- Falta de mecanismos de identificación y autenticación	T5

6.2.4.- IDENTIFICACIÓN DE AMENAZAS

La información sobre amenazas puede obtenerse de los incidentes pasados, duelos de activos, usuarios y otras fuentes incluyendo especialistas de seguridad, autoridades, catálogos de amenazas externas, estadísticas, etc.

Las amenazas pueden ser deliberadas, accidentales o ambientales (naturales). Ej. Robo de información, falla de equipo, sismo, etc.
Debe también identificarse el tipo y fuente de amenaza

Agente de Amenaza.- Una entidad puede actuar o causar que un evento de amenaza ocurra al explotar una o más vulnerabilidades en un sistema.

Evento de Amenaza.- Un evento cuya ocurrencia causará daño a un sistema mediante su divulgación, modificación, destrucción y/o negación de servicio. **(Véase Ilustración No.49)**

Proceso: Titularización de Cartera
Actividad: Ingreso de los aspectos legales y financieros
Activo: Base de datos de activos financieros

ILUSTRACIÓN 49 CUADRO DE AMENAZAS EN LOS ACTIVOS DE INFORMACIÓN, AGENTE Y TIPO

	FUENTE (AGENTE)	AMENAZAS(EVENTO)	TIPO
T1	Intruso interno o externo	Abuso de privilegios	Software Información
T2	Intruso interno o externo	Abuso de privilegios	Software
T3	Intruso interno o externo	Abuso de privilegios	Software
T4	Aplicación	Error en el uso	Software
T5	Intruso interno o externo	Suplantación de identidad	Software

6.2.5.- IDENTIFICACION DE CONSECUENCIAS

Esta actividad identifica los daños o consecuencias a la organización causados por un escenario de incidente, tomando en cuenta las consecuencias que puede traer al activo la pérdida de confidencialidad, integridad y disponibilidad.

El impacto de los escenarios de incidente debe ser consistente con los criterios de impacto definidos. Un impacto puede tener efectos inmediatos (operacionales) o futuros (del negocio).

Ejemplos: pérdida de efectividad, condiciones operativas adversas, pérdidas del negocio, daño a la reputación, etc. **(véase Ilustración No.50)**

Proceso: Titularización de Cartera
Actividad: Ingreso de los aspectos legales y financieros
Activo: Base de datos de activos financieros

ILUSTRACIÓN 50 CUADRO DE ESCENARIO: AMENAZAS, VULNERABILIDADES Y CONSECUENCIAS

ESCENARIOS			
	AMENAZA	**VULNERABILIDAD**	**CONSECUENCIAS/IMPACTOS**
S1	Abuso de privilegios	Fallas conocidas en el software	Uso no autorizados, Integridad
S2	Abuso de privilegios	Falta de pistas de auditoría	Integridad, fraude
S3	Abuso de privilegios	Incorrecta asignación de privilegios de acceso	Integridad, Fraude y Uso no autorizado
S4	Error en el uso	Falta de documentación	Interrupción del negocio, Uso no autorizado, brechas de desempeño
S5	Suplantación de identidad	Falta de mecanismos de identificación y autenticación	Impacto legal, regulaciones, cumplimiento, integridad, uso no autorizado

6.3.- HERRAMIENTA DE ANÁLISIS DE LOS RIESGOS

Para la aplicación de este caso práctico se utilizará la metodología del marco de referencia NIST SP 800-30, previo a utilizar esta técnica es preciso establecer los siguientes delineamientos tendientes a situarnos en la realidad de la institución a analizar. Considerando los 15 principales activos de información necesarios para el desarrollo de las principales actividades dentro del proceso de titularización de cartera de la empresa del mercado de valores ecuatoriano.

Para lo cual se utilizará el procedimiento de administración de riesgos de seguridad de la información diagramado en este cuadro de actividades **(Véase Ilustración No.51)**

ILUSTRACIÓN 51 CUADRO DE PROCEDIMIENTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
Responsable del Sistema de Gestión	1	Convoca a los Dueños de procesos a la reunión para llevar a cabo el proceso de administración del riesgo.		
Dueños de procesos	2	Asisten a la reunión de administración del riesgo convocada por el Responsable del Sistema de Gestión.		
Dueños de procesos	3	Identifican los activos de información a ser incluidos en el Análisis de Riesgos de Información con base en la información contenida en los inventarios de información de cada área de acuerdo a lo definido en el Inventario de Activos de Información y se documentan en el campo 2 (Activo) del formato Análisis de Riesgos de Información.		Formato de Inventario de Activos de Información Formato de Análisis de Riesgos de Información
Dueños de procesos	4	Identifican las amenazas que afectan a los activos de información identificados y se documentan en el campo 3 (Amenaza) del Análisis de Riesgos de Información.		Formato de Análisis de Riesgos de Información
Dueños de procesos	5	Identifican las vulnerabilidades a las que están expuestos los activos de información identificados y se documentan en el campo 4 (Vulnerabilidad) del Análisis de Riesgos de Información.		Formato de Análisis de Riesgos de Información
Dueños de procesos	6	Asignan un número de identificación consecutivo al conjunto AAV y se documenta en el campo 1 (ID) del Análisis de Riesgos de Información.)		Formato de Análisis de Riesgos de Información
Dueños de	7	Califican la probabilidad de ocurrencia del conjunto AAV seleccionándola de la lista		Formato de Análisis de Riesgos de

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
procesos		despegable del campo 6 (Probabilidad) del Análisis de Riesgos de Información; para lo cual se toma en cuenta los siguientes parámetros: • ***N/A:*** Es improbable que se dé la ocurrencia del conjunto AAV • ***BAJO:*** El conjunto AAV ha ocurrido una vez durante toda la vida del Activo • ***MEDIO:*** El conjunto AAV ha ocurrido una vez durante el último año • ***ALTO:*** El conjunto AAV ha ocurrido más de una vez durante el último año		Información
Dueños de procesos	8	Califican la consecuencia de la ocurrencia de la amenaza sobre el activo seleccionándola de la lista despegable del campo 7 (Consecuencia) del Análisis de Riesgos de Información, para lo cual se toma en cuenta los siguientes parámetros: • ***N/A:*** La ocurrencia de la amenaza sobre el activo no tiene consecuencias • ***BAJO:*** La ocurrencia de la amenaza sobre el activo pone en riesgo información pública • ***MEDIO:*** La ocurrencia de la amenaza sobre el activo pone en riesgo información interna • ***ALTO:*** La ocurrencia de la amenaza sobre el activo pone en riesgo información confidencial		Formato de Análisis de Riesgos de Información
Dueños de procesos	9	Califican la dificultad de acceso al activo de información seleccionándola de la lista despegable del campo 8 (Dificultad de acceso al Activo) del Análisis de Riesgos de Información , para lo cual se toman en cuenta los siguientes parámetros: • ***N/A:*** La ocurrencia del conjunto AAV es improbable • ***BAJO:*** No existen condiciones especializadas para poder acceder al Activo o no cuenta con elementos de protección o controles implementados, el Activo esta siempre en condiciones de ser explotado por alguna amenaza • ***ALTO:*** Existen condiciones especializadas		Formato de Análisis de Riesgos de Información

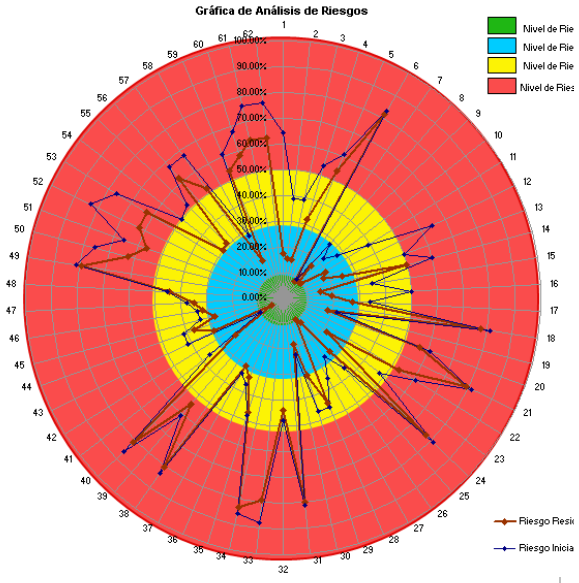
Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
		para poder tener acceso al Activo, se cuentan con controles y/o elementos de protección establecidos.		
Dueños de procesos	10	Califican en qué grado afecta la ocurrencia del conjunto AAV a la confidencialidad de la información seleccionándolo de la lista despegable del campo 9 (Confidencialidad) del Análisis de Riesgos de Información, para lo cual se toman en cuenta los siguientes parámetros: • ***NINGUNA:*** No tiene impacto sobre la confidencialidad de la información • ***PARCIAL:*** Exposición considerable de la información, acceso a sistemas o archivos confidenciales y/o internos. • ***COMPLETA:*** Pérdida completa de la protección, lo cual resulta en la revelación de información confidencial.		Formato de Análisis de Riesgos de Información
Dueños de procesos	11	Califican en qué grado afecta la ocurrencia del conjunto AAV a la integridad de la información seleccionándolo de la lista despegable del campo 10 (Integridad) del Análisis de Riesgos de Información, para lo cual se toman en cuenta los siguientes parámetros: • ***NINGUNA:*** No tiene impacto sobre la integridad de la información • ***PARCIAL:*** Considerable brecha en la integridad. Es posible la modificación de información. • ***COMPLETA:*** La integridad se ve totalmente comprometida. La información es totalmente manipulada.		Formato de Análisis de Riesgos de Información
Dueños de procesos	12	Califican en qué grado afecta la ocurrencia del conjunto AAV a la disponibilidad de la información seleccionándolo de la lista despegable del campo 11 (Disponibilidad) del Análisis de Riesgos de Información, para lo cual se toman en cuenta los siguientes parámetros: • ***NINGUNA:*** No tiene impacto sobre la disponibilidad de la información		Formato de Análisis de Riesgos de Información

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
		• ***PARCIAL:*** Interrupción considerable en la disponibilidad de los recursos y/o activo de información. • ***COMPLETA:*** Total indisponibilidad de los recursos y/o activo de información.		
Dueños de procesos	13	Asignan una ponderación dependiendo de la característica de la información que se vea más afectada, seleccionándolo de la lista despegable del campo 12 (Ponderación de CID) del Análisis de Riesgos de Información , para lo cual se toman en cuenta los siguientes parámetros: • ***NORMAL:*** Las tres características de la información CID se ven afectadas de igual manera. • ***CONFIDENCIALIDAD:*** La confidencialidad se ve afectada en mayor grado que la integridad o la disponibilidad • ***INTEGRIDAD:*** La integridad se ve afectada en mayor grado que la confidencialidad o la disponibilidad • ***DISPONIBILIDAD:*** La disponibilidad se ve afectada en mayor grado que la integridad o la confidencialidad		Formato de Análisis de Riesgos de Información
Dueños de procesos	14	Califican la complejidad para explotar la amenaza identificada en el conjunto AAV, seleccionándolo de la lista despegable del campo 13 (Explotación de la amenaza) del Análisis de Riesgos de Información, para lo cual se toman en cuenta los siguientes parámetros: • ***NO PROBADA:*** No existe información disponible sobre cómo explotar la amenaza • ***PRUEBA DE CONCEPTO:*** Existen pruebas a nivel de ambiente controlado o de laboratorio sobre cómo explotar la amenaza, pero no ha sido probado en ambientes reales o de operación. • ***FUNCIONAL:*** La amenaza ha sido por medio de un procedimiento o de un mecanismo automatizado en circunstancias, lugares o eventos pero no ha sucedido en el conjunto AAV identificado		Formato de Análisis de Riesgos de Información

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
		• ***PROBADA:*** La amenaza ya ha sido explotada para el conjunto AAV identificado		
Dueños de procesos	15	Determinan el tipo de control que se le ha dado a la ocurrencia del conjunto AAV para mitigar el posible impacto, seleccionándolo de la lista despegable del campo 14 (Control Implementado) del Análisis de Riesgos de Información , para lo cual se toman en cuenta los siguientes parámetros: • ***PERMANENTE:*** Se ha implementado un control de manera permanente • ***TEMPORAL:*** Por el momento se tiene un control temporal pero no será de manera permanente • ***INMEDIATO:*** Control dado de manera inmediata para contener el impacto de la ocurrencia del conjunto AAV • ***NINGUNO:*** No se ha implementado ningún control		Formato de Análisis de Riesgos de Información
Dueños de procesos	16	Determinan la severidad de la amenaza reportada, seleccionándolo de la lista despegable del campo 15 (Reporte de la amenaza) del Análisis de Riesgos de Información , para lo cual se toman en cuenta los siguientes parámetros: • ***NO CONFIRMADO:*** Existe poca confiabilidad sobre la validez del reporte de la amenaza (fuente no confiable, rumor, radio pasillo, etc.) • ***IDENTIFICADO:*** Múltiples fuentes reportan la existencia de la amenaza o múltiples áreas tienen la misma versión, pero no se ha reconocido por el responsable del activo. • ***CONFIRMADO:*** Ha sido oficialmente reportada y confirmada la existencia de la amenaza hacia el activo.		Formato de Análisis de Riesgos de Información
Dueños de procesos	17	Calculan y documentan en el campo 16 (Riesgo Inicial) del Análisis de Riesgos de Información, el riesgo inicial del conjunto AAV, identificando el nivel de riesgo de		Formato de Análisis de Riesgos de Información

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
		acuerdo al siguiente código de colores: • ***VERDE (RIESGO BAJO):*** El riesgo inicial se encuentra entre 0% y 10% • ***AZUL (RIESGO MEDIO):*** El riesgo inicial es mayor que 10% y menor o igual a 30% • ***AMARILLO (RIESGO ALTO):*** El riesgo inicial es mayor que 30% y menor o igual a 50% • ***ROJO (RIESGO MUY ALTO):*** El riesgo inicial es mayor a 50 %[69]		
Dueños de procesos	18	Calculan y documentan en el campo 17 (Riesgo Residual) del Análisis de Riesgos de Información, el riesgo residual del conjunto AAV, identificando el nivel de riesgo de acuerdo al siguiente código de colores: • ***VERDE (RIESGO BAJO):*** El riesgo residual se encuentra entre 0% y 10% • ***AZUL (RIESGO MEDIO):*** El riesgo residual es mayo a 10% y menor o igual a 30% • ***AMARILLO (RIESGO ALTO):*** El riesgo residual es mayor a 30% y menor o igual a 50% • ***ROJO (RIESGO MUY ALTO):*** El riesgo residual es mayor a 50%		Formato de Análisis de Riesgos de Información
Dueños de procesos	19	Obtienen una gráfica de radar en donde se grafican riesgo inicial y riesgo residual obtenido, en donde se maneja los mismos niveles de riesgo de los pasos anteriores, como la que se muestra a continuación:		Formato de Análisis de Riesgos de Información

[69] Dr. Jorge Garibay, metodología de Redit

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
				
Dueños de procesos	20	Identifican los controles aplicables del “Anexo A” de ISO 27001:2005 para mitigar el conjunto AAV identificado y se documente en el campo 5 (Control ISO 27001) del Análisis de Riesgos de Información.		Formato de Análisis de Riesgos de Información
Responsable del Sistema de Gestión	21	Crea o actualiza la Declaración de Aplicabilidad (SoA), tomando como base los resultados obtenido en el proceso de Administración del Riesgo para justificar la selección o exclusión de controles.		Declaración de Aplicabilidad
Responsable del Sistema de Gestión	22	Para los riesgos residuales que no estén dentro del nivel aceptado por la Dirección General se crea un Plan de Tratamiento de Riesgos en el cual se incluye al menos: • ID Riesgo • Riesgo • Acciones de tratamiento • Riesgo a Tratar • Riesgo Residual Estimado • Responsable implementación • Recursos • Tiempo compromiso • Inversión requerida		Formato de Plan de Tratamiento de riesgos

Responsable	No. Act	Actividades	Duración	E/S Formatos/ Lineamiento
Responsable del Sistema de Gestión	23	Presenta los resultados del Análisis de Riesgos de Información y el Plan de Tratamiento de Riesgos al Comité Directivo para su aprobación.		Formato de Análisis de Riesgos de Información Formato de Plan de Tratamiento de Riesgos
Comité Directivo		Aprueba el Plan de Tratamiento de Riesgos		Formato de Plan de Tratamiento de Riesgos
Responsable del Sistema de Gestión		Comunica a los Dueños de procesos los resultados obtenidos de la ejecución de este procedimiento.		Análisis de Riesgos Formato de Plan de Tratamiento de Riesgos
Dueños de procesos		Difunden los resultados obtenidos de la ejecución de la este procedimiento al personal a su cargo. Termina Procedimiento.		Análisis de Riesgos

Realizado el correspondiente procedimiento de análisis de riesgos de seguridad de la información apoyándonos en un cuadro de Excel detallando paso a paso, se tiene que tener presente que el riesgo puede convertirse en una ventaja competitiva para la organización siendo capaces de gestionarlo adecuadamente. La capacidad de gestionar convenientemente un elevado nivel de riesgo puede ser un factor diferenciador en la medida en que (JoneS05A) (UNE71504.08):

- La Organización puede operar en circunstancias en las que otras organizaciones no podrían operar con suficiente seguridad. Con frecuencia, la asunción de un mayor nivel de riesgo lleva asociada un mayor retorno de la inversión, que podría denominarse una ¨prima de riesgo¨.

- El mejor control del riesgo permite a la Organización disponer de información de mejor calidad para la toma de decisiones. Por ejemplo, la capacidad de valorar el nivel de riesgo puede permitir determinar si la ¨prima de riesgo¨ es proporcionada y justificada la asunción de un riesgo adicional.

- El mejor control del riesgo también permite detectar de forma inmediata las desviaciones, proporcionando un mayor tiempo de reacción para la toma de medidas correctoras. Por ejemplo, la detección anticipada del mal funcionamiento de un determinado procedimiento de soporte (o de un cambio en el entorno que pueda afectar el proceso) puede permitir la introducción de controles adicionales, de modo que las deficiencias se corrijan antes de que el impacto sea significativo.

- Por último, un mejor control del riesgo, en la medida en que pueda comunicarse a todos los grupos de interés (accionistas, personal, clientes, proveedores, supervisores, etc.) puede dar ventajas competitivas significativas (mayor acceso a la financiación, facilidad para retener el talento, facilidad para lograr fidelizar clientes, etc.) **(véase Ilustración No.52)**

ILUSTRACIÓN 52 HERRAMIENTA DE ANÁLISIS TOTAL DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN EXCEL

ANALISIS DE RIESGOS

Área: TITULARIZACIÓN DE CARTERA

Fecha: oct-11

Nivel de Riesgo Aceptado: 30,00%

ID	Activo	Amenaza	Vulnerabilidad	Control ISO 27001	Probabilidad	Consecuencia	Prob	Impacto	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID		Explotación de la amenaza	Control Implementado	Reporte de la amenaza		Riesgo Inicial	Riesgo Residual
1	Servidores	Falta de replica de respaldos	En caso de falla del dispositivo de respaldos (robot) o en un escenario de contingencia los tiempos de recuperación serían mayores	A.10.5.1, A.14.1.2	BAJO	MEDIO	0,15	0,50	ALTO	COMPLETA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,81	PRUEBA DE CONCEPTO	INMEDIATO	IDENTIFICADO	0,23	41,82%	15,22%
		Brechas de mantenimiento del sistema de información	Mantenimiento insuficiente/instalación fallida de medios de almacenamiento	A.9.2.4, A.10.7.3	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,70	PRUEBA DE CONCEPTO	INMEDIATO	IDENTIFICADO	0,23	37,22%	14,15%
		Polvo corrosión	Susceptible a humedad,polvo	A.9.2.1, A.14.1.1	BAJO	MEDIO	0,15	0,50	ALTO	PARCIAL	NINGUNA	PARCIAL	DISPONIBILIDAD	0,50	PRUEBA DE CONCEPTO	INMEDIATO	NO CONFIRMADO	0,30	28,70%	13,86%
		Pérdida de alimentación eléctrica	Susceptible a variaciones de voltaje	A.7.1.2, A.9.2.3	MEDIO	ALTO	0,90		ALTO	COMPLETA	PARCIAL	COMPLETA	DISPONIBILIDAD	0,88	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	84,54%	68,79%
2	Equipos de escritorio ,portátiles y dispositivos de almacenamiento	Destrucción del equipo y medios	Falta de esquemas de reemplazo periódico	A.7.1.3, A.14.1.5	ALTO	ALTO	0,90		ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	0,33	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	80,99%	78,52%
		Error en el uso	Falta de eficiente control de cambios en la configuración	A.6.1.4, A.14.1.5	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	NINGUNA	CONFIDENCIALIDAD	0,53	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	29,91%	17,54%
		Fenómenos meteorológicos	Susceptible a variaciones de temperatura	A.9.2.1, A.14.1.2	BAJO	ALTO	0,15	0,90	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	0,48	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	43,84%	29,85%
3	Contraseñas de empleados	Posibilidad de acceso por personal externo en cualquier momento y desde cualquier ubicación (Suplantación de Identidad)	Falta de mecanismos de identificación y autenticación	A.10.1.3, A.11.2.3	BAJO	MEDIO	0,15	0,50	ALTO	COMPLETA	PARCIAL	NINGUNA	CONFIDENCIALIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,25%	20,88%
		Violación de los sistemas provocando la pérdida o modificación de los datos sensibles de la organización	Pobre gestión de claves secretas	A.10.10.2 y A.11.2.3	MEDIO	ALTO	0,90		ALTO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,66	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	74,80%	58,43%
		Utilización de una misma contraseña en múltiples sistemas	Falta de registro y control de todos de claves secretas(desprotegidos)	A.10.10.3, A.11.2.3	MEDIO	MEDIO	0,50		BAJO	COMPLETA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,85	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	46,25%	34,56%
	Medios extraíbles(por ejemplo, CD-ROM,DVD,discos duros portátiles, dispositivos de almacenamiento	Brechas de mantenimiento del sistema de información	Instalación fallida de medios de almacenamiento	A.10.7.3 y A.10.10.5	MEDIO	MEDIO	0,50		BAJO	PARCIAL	COMPLETA	PARCIAL	INTEGRIDAD	0,85	FUNCIONAL	PERMANENTE	NO CONFIRMADO	0,20		

5	Fuentes de información de contratos con socios	Abuso de privilegios	Falta de pistas de auditoria	A.10.10.1 y A.11.5.2	BAJO	MEDIO	0,15	0,50	ALTO	COMPLETA	PARCIAL	NINGUNA	CONFIDENCIALIDAD	0,64	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	34,72%	19,76%
			Incorrecta asignación de privilegios de accesos	A11.2.2, A.11.4.2	BAJO	MEDIO	0,15	0,50	ALTO	PARCIAL	PARCIAL	NINGUNA	CONFIDENCIALIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	28,70%	17,04%
		Corrupción de datos	Software ampliamente distribuido	A.10.8.1, A.12.5.3	BAJO	ALTO	0,15	0,90	ALTO	PARCIAL	PARCIAL	NINGUNA	INTEGRIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	51,68%	30,67%
			Aplicación de programas de datos erróneos en términos de tiempo	A.10.4.1,A.12.5.2	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,25%	20,83%
		Procesamiento ilegal de datos	Servicios innecesarios habilitados	A.6.1.4, A.14.1.5	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	INTEGRIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,25%	20,83%
		Pérdida de información	Falta de copias de respaldo	A.10.5.1, A.14.1.2	BAJO	ALTO	0,15	0,90	BAJO	COMPLETA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,85	FUNCIONAL	PERMANENTE	IDENTIFICADO	0,15	78,53%	23,25%
6	Personal Operativo del sistema financiero	Brechas en la disponibilidad de personal	Ausencia de personal debidamente calificado	A.8.1.2,A.13.2.2	MEDIO	MEDIO	##	0,50	ALTO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,47%	30,61%
		Robos de medios o documentos	Trabajo del personal de limpieza no supervisado	A.8.2.1,A.13.2.1	BAJO	ALTO	0,15	0,90	BAJO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,53	FUNCIONAL	INMEDIATO	NO CONFIRMADO	0,60	53,68%	37,60%
		Destrucción del equipo y medios	Procedimientos inadecuados de reclutamiento	A.8.1.2,A.13.2.2	MEDIO	MEDIO	##	0,50	ALTO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,47%	30,61%
		Error en el uso	Entrenamiento de seguridad insuficiente	A.8.2.2,A.13.2.2	MEDIO	MEDIO	##	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	42,50%	32,88%
			Falta de concientización en seguridad	A.8.2.3,A.13.1.2	ALTO	ALTO	##	0,90	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	FUNCIONAL	PERMANENTE	IDENTIFICADO	0,15	85,38%	77,92%
			Falta de mecanismos de monitoreo	A.10.10.2 y A.11.2.3	BAJO	MEDIO	0,15	0,50	BAJO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,53	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	29,61%	17,54%
7	Información financiera cifrada(encriptadas) bursátil de clientes y proveedores	Corrupción de datos	Falta de procedimientos formales para el control de documentos del Sistema de Gestión de Seguridad de la información	A.6.1.2,A.12.3.1	BAJO	ALTO	0,15	0,90	BAJO	COMPLETA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,85	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	78,53%	42,76%
			Falta de procedimientos formales para la Supervisión	A.6.1.3,A.15.1.6	BAJO	ALTO	0,15	0,90	BAJO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,70	FUNCIONAL	NINGUNO	IDENTIFICADO	0,60	67,08%	45,63%
		Denegación de acciones	Falta de asignación apropiada de responsabilidades de seguridad de la información	A.6.1.4,A.12.3.2	MEDIO	MEDIO	##	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	INTEGRIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	42,50%	32,88%
									BAJO	NINGUNA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,85	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	0,00%	0,00%
		Datos de fuentes no confiables	Falta de procesos formales para la autorización de información públicamente disponible	A.7.2.1, A.14.1.5	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,22%	20,87%
									BAJO	COMPLETA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,85	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	0,00%	0,00%
		Fallo de equipos	Falta de planes de continuidad	A.12.5.1,A.14.1.3	BAJO	ALTO	0,15	0,90	BAJO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	67,08%	37,60%
		Robos de medios o documentos	Falta de mecanismos de monitoreo establecidos para violaciones de seguridad	A.11.6.1,A.15.2.1	BAJO	ALTO	0,15	0,90	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	67,08%	37,60%
			Falta de autorización de instalaciones de procesamiento de información	A.11.3.3,A.15.1.1	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	PRUEBA DE CONCEPTO	TEMPORAL	IDENTIFICADO	0,15	37,25%	11,96%

8	Sitio Web interno (Intranet)	Datos de fuentes no confiables	Falta de procesos formales para la autorización de información públicamente disponible	A.6.1.1,A.11.4.1	BAJO	MEDIO	0,15	0,50	ALTO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,67	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	35,76%	30,22%
		Abuso de privilegios	Falta de procedimientos formales para el registro y des-registros de usuarios de Intranet	A.8.3.3,A.11.4.5	MEDIO	MEDIO	##	0,50	ALTO	NINGUNA	PARCIAL	PARCIAL	INTEGRIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,47%	30,61%
		Brechas en el mantenimiento de sistemas de información	Mantenimiento del sitio inadecuado	A.10.4.1,A.11.4.7	BAJO	MEDIO	0,15	0,50	BAJO	NINGUNA	PARCIAL	PARCIAL	INTEGRIDAD	0,53	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	29,81%	17,54%
		Abuso de privilegios	Falta de procedimientos formales para la revisión de derechos de acceso(supervisión)	A.10.1.3,A.11.4.2	BAJO	BAJO	0,15	0,20	BAJO	NINGUNA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,35	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	8,35%	5,68%
9	Diseño e Infraestructura de red	Suplantación de identidad	Falta de identificación y autenticación de emisor y receptor	A.10.6.2,A.11.6.1	MEDIO	MEDIO	##	0,50	ALTO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,67	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	41,63%	32,40%
		Saturación de sistemas de información	Inadecuada gestión de riesgos	A.10.6.1,A.11.4.5	MEDIO	MEDIO	##	0,50	ALTO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,66	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	41,61%	32,47%
		Falla de equipos de telecomunicaciones	Cableado unido pobremente	A.9.2.3,A.11.4.6	MEDIO	MEDIO	##	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	42,50%	32,88%
		Espionaje	Tráfico sensible y líneas de comunicación desprotegidas	A.10.9.2,A.11.4.2	BAJO	MEDIO	0,15	0,50	BAJO	COMPLETA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,78	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	40,44%	22,92%
		Espionaje remoto	Arquitectura de red insegura	A.11.4.1, A	MEDIO	MEDIO	##	0,50	BAJO	COMPLETA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,78	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	44,38%	30,72%
		Uso no autorizado de equipo	Conexiones a redes públicas desprotegidas	A.11.4.3,A.10.6.2,	MEDIO	MEDIO	##	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	42,50%	32,88%
10	Centro de datos	Alimentación de energía eléctrica inestable	Pérdida de provisión de energía eléctrica por largos períodos de tiempo	A.14.1.3,A.14.1.5	MEDIO	ALTO	##	0,90	BAJO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	76,50%	59,18%
		Localización en un área susceptible a inundaciones	Inundación	A.9.1.4, A.9.2.1	BAJO	ALTO	0,15	0,90	BAJO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,53	PRUEBA DE CONCEPTO	INMEDIATO	IDENTIFICADO	0,23	53,66%	22,54%
		Dentro del centro de computo labora personal de diversas áreas técnicas.	Manipulación, robo o perdida de información	A.9.1.3,A.15.3.2	BAJO	ALTO	0,15	0,90	BAJO	COMPLETA	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,85	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	78,53%	42,76%
		Acceso no controlado al SITE de personal ajeno a la empresa	Robo de partes y/o equipo	A.9.1.1, A.9.1.2	BAJO	ALTO	0,15	0,90	BAJO	NINGUNA	PARCIAL	PARCIAL	INTEGRIDAD	0,53	FUNCIONAL	PERMANENTE	IDENTIFICADO	0,15	53,66%	19,52%
		Falta de mantenimiento al sistema de aire acondicionado para el cuarto de comunicaciones	Daño o degradación del equipo de cómputo por sobrecalentamiento y/o humedad.	A.9.1.4, A.9.2.4	BAJO	ALTO	0,15	0,90	BAJO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	67,03%	37,60%
		Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador	A.9.1.6,A.15.1.3	MEDIO	MEDIO	##	0,50	ALTO	COMPLETA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,74	PRUEBA DE CONCEPTO	INMEDIATO	IDENTIFICADO	0,23	43,41%	29,14%
11	Base de datos del proceso de titularización de cartera bursátil	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	A.10.10.2 y A.14.1.4	BAJO	MEDIO	0,15	0,50	BAJO	NINGUNA	PARCIAL	PARCIAL	INTEGRIDAD	0,53	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	29,81%	17,54%
		Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia acuerdos de niveles de servicio	A.12.2.2,A.15.1.3	BAJO	MEDIO	0,15	0,50	BAJO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	37,22%	20,87%

12	Correo electrónico	Falta de políticas de uso de correo electrónico	Error en el uso	A.10.8.1, A.10.8.2	MEDIO	BAJO	↕↕	0,20	BAJO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,70	PROBADA	TEMPORAL	IDENTIFICADO	0,38	16,38%	12,52%
13	Sistema Operativo de titularización de cartera	Abuso de privilegios	Falta de control en el cierre de sesión en terminales desatendidas	A.10.3.1,A.11.5.5	MEDIO	MEDIO	↕↕	0,50	ALTO	PARCIAL	PARCIAL	PARCIAL	CONFIDENCIALIDAD	0,67	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	41,63%	32,48%
		Corrupción de datos	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	A.10.3.2,A.11.5.6	BAJO	MEDIO	0,15	0,50	ALTO	COMPLETA	PARCIAL	PARCIAL	INTEGRIDAD	0,74	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	38,73%	21,53%
		Suplantación de identidad	Falta de mecanismos de identificación y autenticación	A.11.5.2,A.11.5.3	BAJO	MEDIO	0,15	0,50	BAJO	COMPLETA	PARCIAL	PARCIAL	DISPONIBILIDAD	0,78	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	40,44%	22,02%
		Mal funcionamiento del software	Especificaciones poco claras o incompletas de los desarrolladores	A.10.8.5,A.12.5.3	BAJO	BAJO	0,15	0,20	BAJO	PARCIAL	PARCIAL	PARCIAL	NORMAL	0,70	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	14,88%	8,35%
14	Aplicaciones financieras proceso titularización de cartera	Abuso de privilegios	Incorrecta asignación de privilegios de accesos	A.9.1.6,A.12.5.4	BAJO	MEDIO	0,15	0,50	ALTO	PARCIAL	PARCIAL	NINGUNA	CONFIDENCIALIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	29,70%	17,04%
		Corrupción de datos	Falta de mantenimiento formales para la supervisión y correcto uso de las aplicaciones financieras	A.12.2.2,A.15.1.3	MEDIO	ALTO	↕↕	0,90	ALTO	PARCIAL	PARCIAL	NINGUNA	CONFIDENCIALIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	67,44%	55,80%
15	Archivos del sistema de titularización de cartera	Error en el uso	Falta de documentación ,parametrización incorrecta y fechas incorrectas	A.12.4.1,A.15.1.3	BAJO	BAJO	0,15	0,20	ALTO	PARCIAL	COMPLETA	NINGUNA	INTEGRIDAD	0,50	FUNCIONAL	INMEDIATO	IDENTIFICADO	0,45	11,48%	6,82%

Podemos observar **(véase Ilustración No.52)** en el desarrollo de la herramienta que el riesgo residual, que es la pérdida anual esperada, el porcentaje es menor al riesgo inicial precisamente porque está mitigado por los controles implantados reduciendo hasta un 60% la degradación en caso de que se materialicen las amenazas. La pérdida anual se calcula teniendo en cuenta:

- El valor de los activos de información
- La exposición de los recursos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación
- La eficacia de los controles implantados o planificados para reducir la frecuencia o el impacto de las amenazas, teniendo en cuenta el grado de implantación que tendrán tras la ejecución del plan de acción.

El análisis de riesgos permite cuantificar cuál es el coste de la inseguridad (riesgo) que asume una Organización en un momento determinado y cómo evoluciona este coste en función de las medidas de seguridad que se implementen. De esta forma el análisis de riesgo permite determinar cuándo una determinada medida de seguridad va a suponer una reducción del riesgo menor que su propio coste y, por tanto, no es aconsejable su implantación desde un punto de vista económico (MAGE06).

Es importante destacar que no se considera posible la reducción del riesgo a 0. El objetivo del análisis y la gestión de riesgos no es la eliminación completa del riesgo, sino su reducción a unos niveles tolerables por la Organización en función de su apetito al riesgo (MAGE06)(JONES05A).

Esta doble faceta del riesgo como amenaza y como oportunidad se refleja en la existencia de dos términos afines utilizados para denominar la cantidad de riesgo que gestionan las organizaciones (JONES05A) (UNE71504.08):

- Se denomina tolerancia al riesgo a la cantidad de riesgo que una Organización es capaz de gestionar.
- Se denomina apetito de riesgo a la cantidad de riesgo que una Organización está dispuesta a gestionar para lograr los objetivos establecidos.

El presupuesto de Seguridad de la Información es limitado para plantear la implantación completa de cualquiera de los marcos de referencia o códigos de buenas prácticas hasta el máximo nivel de cumplimiento. Por este motivo, los responsables de Seguridad de la Información necesitan mecanismos que les faciliten priorizar las medidas a implantar y que les permitan justificar las decisiones tomadas en ese sentido.

La formalización implica que el análisis debe aportar dos características fundamentales:

- Objetividad, en la medida en que diferentes personas, aplicando el mismo procedimiento sobre los mismos datos, deberían obtener resultados idénticos.
- Valoración, de modo que todos los riesgos y los controles potencialmente aplicables para mitigarlos quedan priorizados utilizando una escala que puede ser numérica (en el caso del análisis cuantitativo) o literal (en el caso del análisis cualitativo).

6.4.- PLAN DE RESPUESTA, SEGUIMIENTO Y CONTROL[70]

Una vez analizado los riesgos, sobre los principales activos de información que soportan el proceso de titularización de cartera de la organización se procede a establecer los controles para poder mitigar, aceptar, traspasar, ignorar o eliminar un riesgo de seguridad de tecnología de información para el desarrollo de este proceso se precisan los controles específicos a realizar en cada activo para poder tomar medidas de seguridad de la información tienen un coste asociado a su implementación y a su mantenimiento. Esto es lo que se conoce como el coste de la seguridad como lo estipula (MAGE06) (JONES05A). **(Véase Ilustración No.53)**

[70] http://web.nvd.nist.gov/view/vuln/search-results?query=data+base&search_type=all&cves=on

ILUSTRACIÓN 53 CUADRO DE CONTROLES PARA LAS AMENAZAS Y VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN MÁS RELEVANTES DEL PROCESO DE TITULARIZACIÓN DE CARTERA DE LA EMPRESA DEL MERCADO DE VALORES ECUATORIANO

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
Servidores	Falta de réplica de respaldos	En caso de falla del dispositivo de respaldos (robot) o en un escenario de contingencia los tiempos de recuperación serían mayores	Disponer de copias de backup de la información confidencial de los clientes y del software. La organización: a. Físicamente controla y almacena de forma segura [asignación: la organización define los tipos de medios digitales y no digitales] en [asignación: la organización define las áreas controladas] con [asignación: la organización define las medidas de seguridad]; b. Protege a los medios de información del sistema hasta que los medios de comunicación son destruidos o desinfectados utilizando el equipo aprobado, técnicas y procedimientos
	Brechas de mantenimiento del sistema de información	Mantenimiento insuficiente/Instalación fallida de medios de almacenamiento	Debe de ubicarse el equipo en el lugar donde se pueda realizar mantenimientos para permitir su continua disponibilidad e integridad. Este control, incluyendo las mejoras especificadas, puede ser satisfecho por cumplir requisitos similares por otra entidad de la organización que no sea el programa de seguridad de la información. Organizaciones de evitar la duplicación de acciones ya cubiertas.
	Polvo corrosion	Falta de mantenimiento por lo cual es susceptible a humedad, polvo afectando la disponibilidad e integridad de la información del negocio	El equipo debe de protegerse para reducir los riegos de las amenazas y peligros ambientales. La política de protección del medio ambiente físico y puede ser incluido como parte de la política de seguridad de la información general de la organización. Implementar procedimientos de protección física y ambiental puede ser desarrollado para el programa de seguridad en general y para un determinado sistema de información, cuando sea necesaria(NIST)"

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
Servidores	Pérdida de alimentación eléctrica	Falta de un plan preventivo y remediador a los equipos susceptibles a variaciones de voltaje que ocasionen destrucción, pérdida o corrupción de la información	La organización debe emplear y mantener la planta de iluminación de emergencia automático del sistema de información que se activa en caso de un apagón o interrupción y que cubre las salidas de emergencia y rutas de evacuación dentro de la instalación.
	Incendios	Falta de un plan preventivo o localización de un lugar susceptible a eventos de desastres	Dispositivos de supresión de incendios y detección / sistemas incluyen, por ejemplo, los sistemas de rociadores, extintores portátiles de incendios, mangueras de sistemas fijos de extinción, y detectores de humo. Este control, incluyendo las mejoras especificadas, puede ser satisfecho por cumplir requisitos similares por otra entidad de la organización que no sea el programa de seguridad de la información. Organizaciones de evitar la duplicación de acciones ya cubiertas
2.- Equipos de Escritorio, portátiles y dispositivos de almacenamiento	Destrucción del equipos y medios	Falta de esquemas de reemplazo periódico que impida se vea afectada la disponibilidad e integridad de la información del negocio	Sustituir los componentes del sistema de información, cuando sea necesario, y un mecanismo para el intercambio de roles activos y en espera de los componentes.
	Error en el uso	Falta de eficiente control de cambios en la configuración	La organización debe contar con mecanismos automatizados para: (a) Documento de propuesta de cambios en el sistema de información, (b) Notificar a las autoridades designadas de aprobación; (c) Poner de relieve la aprobación que no han sido recibidos por [asignación: organización periodo de tiempo definido], (d) inhiben el cambio hasta que se reciban las aprobaciones designado, y (e) Documento completado los cambios en el sistema de información.

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
2.- Equipos de Escritorio, portátiles y dispositivos de almacenamiento	Fenómenos meteorológicos	Falta de mantenimiento por lo cual es susceptible a variaciones de temperatura afectando la disponibilidad e integridad de la información del negocio	Los lugares alternativos de trabajo, como, por ejemplo, instalaciones gubernamentales o residencias privadas de los empleados. La organización puede definir diferentes conjuntos de controles de seguridad para sitios específicos de trabajo alternativos o tipos de sitios.
3.- Contraseñas de empleados	Posibilidad de acceso por personal externo en cualquier momento y desde cualquier ubicación (Suplantación de Identidad)	Permite a los a atacantes remotos provocar una denegación de servicio a través de elaborados paquetes VLAN que son procesados por la función napi_reuse_skb, lo que lleva a (1) una pérdida de memoria o (2) corrupción de memoria, una vulnerabilidad diferente a CVE-2011-1478.	Un interruptor físico de software de lectura que los comandos de circunvalación de la funcionalidad de acceso y está protegido contra uso accidental o sin supervisión
	Pobre gestión de claves secretas Violación de los sistemas provocando la pérdida o modificación de los datos sensibles de la organización	Permite a los atacantes remotos la violación de los sistemas provocando la pérdida o modificación de los datos sensibles de la organización	La política de control de acceso pueden ser incluidos como parte de la política de seguridad de la información general de la organización. Procedimientos de control de acceso pueden ser desarrollados para el programa de seguridad en general y para un determinado sistema de información, cuando sea necesario. La estrategia de gestión de riesgos de la organización es un factor clave en el desarrollo de la política de control de acceso.
	Falta de registro y control de tablas de claves secretas(desprotegidos)Utilización de una misma contraseña en múltiples sistemas	Utilización de una misma contraseña en múltiples sistemas	La organización debe de: (a) Permitir el uso de autenticadores grupo sólo cuando se utiliza junto con un autenticador individual / único, y (b) requiere que los individuos se autentique con un autenticador individuales antes de utilizar un autenticador de grupo
4.- Medios extraíbles (por ejemplo, CD-ROM. DVD. Discos duros portátiles, dispositivos de almacenamiento USB,etc)	Brechas de mantenimiento del sistema de información	Instalación fallida de medios de almacenamiento	La organización debe: a. Físicamente controla y almacena de forma segura [asignación: la organización define los tipos de medios digitales y no digitales] organización define las áreas controladas] con [asignación: la organización define las medidas de seguridad];

ACTIVO	AMENAZA	VULNERABILIDAD	CONTROLES
5.- Fuentes de información de contratos con socios	Robos de medios o documentos	Falta de control de copiado	La organización debe almacenar copias de seguridad del sistema operativo y otro software crítico del sistema de información, así como copias del inventario del sistema de información (incluyendo hardware, software, firmware y componentes) en una instalación separada o en un recipiente resistente al fuego que no se coloca con el sistema operativo.
	Abuso de privilegios	Falta de pistas de auditoria	Una auditoría formal, documentada y la política de rendición de cuentas que se ocupa de propósito, alcance, funciones, responsabilidades, compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento, y b Procedimientos formales y Documentados para facilitar la aplicación de la directiva de auditoría y rendición de cuentas y la auditoría y controles asociados de rendición de cuentas.
		Incorrecta asignación de privilegios de accesos	La organización debe controlar la información de código abierto para pruebas de ex filtración o divulgación no autorizada de información de la organización
	Corrupción de datos Software ampliamente distribuido	Permite a atacantes remotos causar una denegación de servicio (caída) y posiblemente ejecutar código arbitrario a través de mucho tiempo (1) dominio, NIST	El sistema de información debe: a. Identificar potencialmente relevantes para la seguridad condiciones de error b. Generar mensajes de error que proporcionan la información necesaria para las acciones correctivas sin Revelar [Asignación información de la organización definidos sensibles o potencialmente dañinos] en los registros de mensajes de error y administrativa que podría ser explotado por sus adversarios, y c. Revela los mensajes de error sólo al personal autorizado.

ACTIVO	AMENAZA	VULNERABILIDAD	CONTROLES
5.- Fuentes de información de contratos con socios	Corrupción de datos Software ampliamente distribuido	Aplicación de programas de datos erróneos en términos de tiempo	El sistema de información debe: a. Identificar potencialmente relevantes para la seguridad condiciones de error b. Generar mensajes de error que proporcionan la información necesaria para las acciones correctivas sin revelar los registros de mensajes de error y administrativa que podría ser explotado por sus adversarios, y c. Revelar los mensajes de error sólo al personal autorizado.
	Procesamiento Ilegal de datos	Servicios innecesarios habilitados	La organización debe limitar la capacidad de información de entrada al sistema de información al personal autorizado.
	Pérdida de información	Falta de copias de respaldo	La organización debe: a. Proteger el sistema de información de los daños teniendo en cuenta el tiempo medio de fallo de [asignación: la organización se define la lista de los componentes del sistema de información] en entornos específicos de la operación, y b. Ofrecer sustituir los componentes del sistema de información, cuando sea necesario, y un mecanismo para el intercambio de roles activos y en espera de los componentes
6.- Personal Operativo del sistema financiero	Brechas en la disponibilidad de personal	Ausencia de personal debidamente calificado	La organización debe establecer como control: a. Pantallas de los individuos antes de autorizar el acceso al sistema de información, y b. Rescreens individuos de acuerdo a [asignación: la organización se define la lista de condiciones que requieren nuevos controles y, si es tan re-examen indicado, la frecuencia de estos nuevos controles]. Medidas de desempeño son las métricas basadas en resultados que utiliza una organización para medir la eficacia o eficiencia del programa de seguridad de la información y los controles de seguridad empleadas en apoyo del programa.

ACTIVO	AMENAZA	VULNERABILIDAD	CONTROLES
6.- Personal Operativo del sistema financiero	Robos de medios o documentos	Trabajo del personal de limpieza no supervisado	La organización debe autorizar el acceso físico a las instalaciones donde reside basa el sistema de información sobre la posición o rol. La organización debe de exigir dos formas de identificación para tener acceso a las instalaciones donde reside el sistema de información. Ejemplos de formas de identificación tarjeta de identificación, tarjeta, PIN cifrado y biometría.
	Destrucción del equipo y medios	Procedimientos Inadecuados de reclutamiento	La organización debe contar con los siguientes requisitos y / o especificaciones, explícitamente o por referencia, en los contratos de contratación de personal el sistema sobre la base de una evaluación de riesgos y de acuerdo con las leyes federales, órdenes ejecutivas, directivas, políticas, reglamentos y normas: a. La seguridad funcional de las necesidades / especificaciones; b. Relacionados con la seguridad los requisitos de documentación, y c. Desarrollo y evaluación relacionados con los requisitos de seguridad.
	Error en el uso	Entrenamiento de Seguridad insuficiente	La organización deberá de tener: a. Documentos y monitores individuales del sistema de información de seguridad, incluyendo las actividades de formación capacitación básica acerca de la seguridad y la formación específica del sistema de información de seguridad, y b. Conserva los registros individuales de formación para [Asignación: período de tiempo definido por la organización].

ACTIVO	AMENAZA	VULNERABILIDAD	CONTROLES
6.- Personal Operativo del sistema financiero	Error en el uso	Falta de concientización en seguridad	La organización debe desarrollar, diseminar y realizar revisiones / actualizaciones [asignación: la organización se define la frecuencia]: a. Un conocimiento formal, documentada y la seguridad política de formación que se ocupa de propósito, alcance, funciones, responsabilidades, compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento, y b. Procedimientos formales y documentados para facilitar la aplicación de la concienciación sobre la seguridad y la política de formación y sensibilización de seguridad y controles asociados de formación.
		Falta de mecanismos de monitoreo	La organización debe: a. Controlar el acceso físico al sistema de información para detectar y responder a incidentes de seguridad física; b. Opiniones de los registros de acceso físico [asignación: la organización se define la frecuencia], y c. Coordina los resultados de los exámenes e investigaciones con la capacidad de respuesta de las organizaciones de incidente.
7.- Información financiera cifrada(encriptado) bursátil de clientes y proveedores	Corrupción de datos	Falta de procedimientos formales para el control de documentos del Sistema de Gestión de Seguridad de Información	La organización: debe de: Documentar y monitorear individuales del sistema de información de seguridad, incluyendo las actividades de formación capacitación básica acerca de la seguridad y la formación específica del sistema de información de seguridad, y b. Conserva los registros individuales de formación para [Asignación: período de tiempo definido por la organización].

ACTIVO	AMENAZAS	VULNERABILIDADES	CONTROLES
7.- Información financiera cifrada(encriptado) bursátil de clientes y proveedores			Direcciones de mantener esencial misiones y funciones de negocios a pesar de una interrupción del sistema de información, compromiso, o el fracaso; - Direcciones eventual restauración, sistema completo de información, sin deterioro de las medidas de seguridad originalmente planificado y ejecutado, y - es revisado y aprobado por los funcionarios designados dentro de la organización; b. Distribuye copias del plan de contingencia para [Asignación: Lista de organización definida de personal de contingencia clave (identificada por su nombre y / o papel) y elementos de la organización]; c. Coordina las actividades de planificación para imprevistos en las actividades de manejo de incidentes; d. Revisa el plan de contingencia para el sistema de información [asignación: la organización se define la frecuencia], e. Revisa el plan de contingencia para hacer frente a cambios en la organización, sistema de información, o el medio ambiente de operación y los problemas encontrados durante la ejecución del plan de contingencia, la ejecución, o la prueba, y f. Comunica los cambios del plan de contingencia.
	Robos de medios o documentos	Falta de mecanismos de monitoreo establecidos para violaciones de seguridad	La organización debe de contar con un proceso formal de sanciones para el personal que no cumplan con lo establecido políticas de información y procedimientos de seguridad.
		Falta de autorización de instalaciones de procesamiento de información	La organización debe de contar con herramientas automatizadas que notificar a las personas designadas al descubrir discrepancias durante la verificación de la integridad.__El sistema de información detecta cambios no autorizados de software e información.

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
8.- Sitio Web interno (Intranet)	Datos de fuentes no confiables	Falta de procesos formales para la autorización de información públicamente disponible	La organización debe: desarrolla, disemina y revisiones / actualizaciones [asignación: la organización se define la frecuencia]: a. Una formal, documentado el riesgo de que las direcciones de la política de evaluación objetivo, alcance, funciones, responsabilidades, compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento, y b. Procedimientos formales y documentados para facilitar la aplicación de la política de evaluación de riesgos y controles asociados a la evaluación de riesgos
	Abuso de privilegios	Falta de procedimientos formales para el registro y des-registros de usuarios de Intranet	La organización desarrolla, disemina y revisiones / actualizaciones [asignación: la organización se define la frecuencia]: a. Un sistema formal, documentada y de comunicación que se ocupa de la protección de propósito, alcance, funciones, responsabilidades, compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento, y b. Procedimientos formales y documentados para facilitar la aplicación del sistema y la política de protección de las comunicaciones y sistemas relacionados y controla las comunicaciones de protección
	Brechas en el mantenimiento de sistemas de información	Mantenimiento del Sitio Inadecuada	La organización debe de: a. Contar con mecanismos de protección contra el spam en la entrada del sistema de información y puntos de salida y en las estaciones de trabajo, servidores o dispositivos de informática móvil en la red para detectar y actuar sobre los mensajes no solicitados transportados por correo electrónico, archivos adjuntos de correo electrónico, acceso web u otros medios comunes, y b. Actualizaciones de los mecanismos de protección de spam (incluyendo las definiciones de la firma), cuando las nuevas versiones están disponibles de acuerdo con la política de seguridad.

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
			y la información que procesa, almacena o transmite; b. Documentos de los resultados de evaluación de riesgos en [Selección: plan de seguridad, el informe de evaluación de riesgos; Asignación [: organización definida por el documento]]; c. Opiniones de los resultados de la evaluación del riesgo [de asignación: la frecuencia definida por la organización], y d. Actualización de la evaluación del riesgo [de asignación: la organización se define la frecuencia], o cuando hay cambios significativos en el sistema de información o el medio ambiente de operación (incluyendo la identificación de nuevas amenazas y vulnerabilidades), u otras condiciones que pueden afectar el estado de seguridad del sistema
9.-Diseño e Infraestructura de red	Falla de equipos de telecomunicaciones	Cableado unido pobremente	La organización debe de contar con rutas de alimentación redundante y paralelo de cableado. la organización cuenta con controles automáticos de tensión para [asignación: la organización se define la lista de los componentes críticos del sistema de información].
	Espionaje	Tráfico sensible y líneas de comunicación desprotegidas	La organización establece los servicios alternativos de telecomunicaciones, incluyendo los acuerdos necesarios para permitir la reanudación de las operaciones del sistema de información para las misiones y funciones esenciales de negocio dentro de [Asignación: organización periodo de tiempo definido] cuando las capacidades de telecomunicaciones primaria no están disponibles.

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
	Espionaje remoto	Arquitectura de red insegura	Establecer el servicio de resolución de direcciones para una organización son tolerantes a fallos y poner en práctica la separación de roles internos / externo. Para eliminar los puntos únicos de fallo y para mejorar la redundancia, normalmente hay al menos dos sistemas de autoridad de nombres de dominio (DNS), uno configurado como principal y el otro como secundario. Además, los dos servidores se ubican normalmente en dos subredes diferentes y geográficamente separadas (es decir, no se encuentra en el mismo espacio
10.- Centro de Datos	Uso no autorizado de equipo	Conexiones a redes públicas desprotegidas	La organización debe de emitir certificados de claves públicas en un [Asignación: organización política definida por el certificado] u obtiene certificados de clave pública en una política correspondiente certificado de un proveedor de servicios aprobado.
	Alimentación de energía eléctrica inestable	Pérdida de provisión de energía eléctrica por largos períodos de tiempo	La organización de contar con rutas de alimentación redundante y paralelo de cableado. La organización protege a los equipos de alimentación y el cableado para el sistema de información de los daños y la destrucción. Debe de contar con controles automáticos de tensión para [asignación: la organización se define la lista de los componentes críticos del sistema de información
	Localización en un área susceptible a inundaciones	Inundación	La organización identifica un sitio de procesamiento alterno que está separado del sitio de procesamiento primario, para no ser susceptibles a los mismos peligros.

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
10.- Centro de datos	Dentro del centro de cómputo labora personal de diversas áreas técnicas.	Manipulación, robo o pérdida de información, Aplicación en el kernel de Linux 2.6.18 en Red Hat Enterprise Linux 5 y 6/2/32 en Red Hat Enterprise Linux 6, que se utiliza en Red Hat Enterprise Virtualization (RHEV) Hypervisor y otros productos, permite a los a atacantes remotos provocar una denegación de servicio a través de elaborados paquetes VLAN que son procesados por la función napi_reuse_skb, lo que lleva a (1) una pérdida de memoria o (2) corrupción de memoria, una vulnerabilidad diferente	La organización: a. Debe de mantener registros de visitantes el acceso a las instalaciones donde reside el sistema de información (a excepción de aquellas áreas dentro de las instalaciones designadas Oficialmente como de acceso público), y b. Revisa los registros de acceso de los visitantes [asignación: la organización se define la frecuencia].
	Robo de partes y/o equipo	Acceso no controlado al SITE de personal ajeno a la empresa	La organización: a. Controla el acceso físico al sistema de información para detectar y responder a incidentes de seguridad física; b. Opiniones de los registros de acceso físico [asignación: la organización se define la frecuencia], y c. Coordina los resultados de los exámenes e investigaciones con la capacidad de respuesta de las organizaciones de incidente.
	Daño o degradación del equipo de cómputo por sobrecalentamiento y/o humedad.	Falta de mantenimiento al sistema de aire acondicionado para el cuarto de comunicaciones.	La organización proporciona un suministro a corto plazo de energía ininterrumpida para facilitar un apagado ordenado del sistema de información en caso de pérdida de la fuente de energía primaria
	Abuso de privilegios	Falta de reportes de falla registrados en bitácoras de administrador y operador	La organización de puestos de componentes de sistemas de información dentro de la instalación para minimizar los daños potenciales de los peligros físicos y del medio ambiente y para reducir al mínimo la posibilidad de que el acceso no autorizado

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
	Eventos sobrenaturales	Falta de un plan de contingencia contra los daños o degradación del equipo de cómputo, Manipulación, robo o pérdida de información causados por eventos sobrenaturales	Los riesgos físicos y ambientales, por ejemplo, inundaciones, incendios, tornados, terremotos, huracanes, actos de terrorismo, vandalismo, pulsos electromagnéticos, interferencias eléctricas y la radiación electromagnética. Siempre que sea posible, la organización también considera que la ubicación o emplazamiento de la instalación con respecto a los riesgos físicos y ambientales. Además, la organización considera que la ubicación de los puntos de entrada físico donde las personas no autorizadas, mientras que no se le concediera el acceso, sin embargo, podría estar en las proximidades del sistema de información y por lo tanto, aumentan las posibilidades de acceso no autorizado a las comunicaciones de la organización (por ejemplo, a través del uso de sniffers inalámbricos o los micrófonos). Este control, incluyendo las mejoras especificadas, puede ser satisfecho por cumplir requisitos similares por otra entidad de la organización que no sea el programa de seguridad de la información. Organizaciones de evitar la duplicación de acciones ya cubiertas.
11.- Base de datos del proceso de titularización de cartera bursátil	Brechas en el mantenimiento de sistemas de información	Falta de procedimientos de control de cambios	La organización debe: desarrollar, disemina y revisiones / actualizaciones [asignación: la organización se define la frecuencia]: a. Una formal, la documentación del sistema de información de mantenimiento política que contemple la finalidad, alcance, funciones, responsabilidades, compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento, y b. Procedimientos formales y documentados para facilitar la aplicación de la política de información de mantenimiento del sistema y los controles asociados a mantenimiento del sistema

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
11.- Base de datos del proceso de titularización de cartera bursátil	Brechas en el mantenimiento de sistemas de información	Falta o insuficiencia acuerdos de niveles de servicio	La organización configura el sistema de información para ofrecer sólo las capacidades esenciales y, específicamente, prohíbe o restringe el uso de las siguientes funciones, puertos, protocolos y / o servicios: [Asignación: organización de la lista definida de funciones prohibidas o restringidas, puertos, protocolos y / o servicios].
	Falta de políticas de Inventario de la CMDB	Falta de componentes del inventario	La organización desarrolla, documentos, y mantiene un inventario de los componentes del sistema de información que: a. Refleja con precisión el actual sistema de información; b. Es compatible con el límite de la autorización del sistema de información; c. Está en el nivel de granularidad se considere necesario para el seguimiento y presentación de informes; d. Incluye [asignación: la organización define las informaciones que considere necesarias para lograr la rendición de cuentas de propiedad efectivos], y e. Está disponible para su revisión y auditoría por parte de funcionarios designados por la organización.
12.-Correo electrónico	Falta de políticas de uso de correo electrónico	Error en el uso	La organización cuenta con mecanismos de cifrado para evitar la divulgación no autorizada de información durante la transmisión a menos que protegidos por [asignación: la organización define las medidas alternativas de física].
13.-Sistema Operativo de titularización de cartera	Abuso de privilegios	Falta de control en el cierre de sesión en terminales desatendidas	La organización: a. Recibe información de las alertas de seguridad del sistema, consejos y directivas de organizaciones externas designadas en forma permanente; b. Genera alertas de seguridad interna, consejos y directivas que considere necesarias; c. Difunde las alertas de seguridad, consejos y directrices a [asignación: Lista de organización definida de personal (identificada por su nombre y / o papel)], y d. Implementa directivas de seguridad.

ACTIVOS	AMENAZAS	VULNERABILIDADES	CONTROLES
13.-Sistema Operativo de titularización de cartera	Corrupción de datos	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	La organización cuenta con mecanismos de cifrado para evitar la divulgación no autorizada de información durante la transmisión a menos que protegidos por [asignación: la organización define las medidas alternativas de física].
14.-Aplicaciones financieras proceso de titularización de cartera	Abuso de privilegios	Incorrecta asignación de privilegios de accesos	La organización: a. Utiliza el software y la documentación asociada, de conformidad con los acuerdos contractuales y las leyes de derechos de autor; b. Cuenta con sistemas de seguimiento para el software y la documentación asociada protegidas por licencias de cantidad para controlar la copia y distribución, y c. Controles y documenta el uso de peer-to-peer para compartir archivos para asegurarse de que esta capacidad no se utiliza para la distribución no autorizada, visualización, ejecución o reproducción de obras protegidas..
	Corrupción de datos	Falta de mantenimiento formales para la supervisión y exacto uso de las aplicaciones financieras	La organización establece las pruebas de los mecanismos de protección de código malicioso [asignación: la organización se define la frecuencia] mediante la introducción de un conocido benigna, la no propagación de casos de prueba en el sistema de información y de verificación de que tanto la detección del caso de prueba e informes.
15.-Archivos del sistema de titularización de cartera	Error en el uso	Falta de documentación, parametrización incorrecta y fechas incorrectas	El sistema de información produce los registros de auditoría que contienen información suficiente para, como mínimo, establecer qué tipo de evento que ocurrió, cuando (fecha y hora) se produjo el evento, donde ocurrió el hecho, el origen del evento, el resultado (éxito o el fracaso del evento, y la identidad de cualquier usuario / objeto asociado al evento.

Es importante señalar que la falta de controles de seguridad también tiene un coste asociado para las organizaciones, en forma de incidentes de seguridad que producen pérdidas. Esto es lo que se conoce el coste de inseguridad (MAGE06)

Los costes de inseguridad también pueden ser directos o indirectos y también pueden ser difíciles de acotar con precisión (MAGE06)

Por ejemplo, el extravío de un soporte con información de solicitudes de clientes puede suponer, entre otros, los siguientes costes:

- Costes directos:
    - Reemplazo del soporte extraviado (generalmente supondrá un coste depreciable)
    - Reemplazo de la información extraviada, bien sea a partir de datos disponibles en la Organización o contactando nuevamente con los clientes.
- Costes indirectos:
    - Costes legales, por incumplimiento de leyes como la Ley de Protección de Datos o los acuerdos de confidencialidad con los clientes.
    - Costos reputacionales, debidos a la pérdida de confianza de los clientes, o del público en general si la noticia tiene una difusión amplia.
    - Costos comerciales, debidos al retraso en el servicio de las solicitudes.
    - Costos de gestión, debido al personal que debe dedicarse a recopilar de nuevo la información perdida y a proceder con el nuevo procedimiento de gestión de las solicitudes.

En síntesis el objetivo de la Organización es minimizar el coste total, tomando como la suma del coste de la seguridad y el coste de la inseguridad (MAGE06).

El establecimiento de procedimientos periódicos de revisión del análisis de riesgos de seguridad de la información. Aunque se lleven a cabo los procedimientos adecuados para la evolución del análisis de riesgos con la evolución de la Organización y de su entorno, es conveniente realizar periódicamente una revisión completa del análisis realizado. Esto se debe a que los procedimientos de actualización continua pueden pasar por alto determinados cambios leves que, sostenidos en el tiempo, pueden terminar impactando sobre la valoración de los riesgos.

También es posible que exista una determinada tasa de errores en la ejecución de los procesos de actualización del análisis de riesgos, provocando una desvirtuación progresiva del análisis de riesgos. Las revisiones periódicas del análisis de riesgos pueden realizarse utilizando la misma metodología empleada en el primer desarrollo, si bien, generalmente, su aplicación podrá ser mucho más ligera, por existir una base de partida importante, si bien esta base deberá utilizarse con cuidado para evitar que su uso introduzca un sesgo en la revisión del análisis. El desarrollo de este procedimiento de revisión debe llevar asociada la asignación de roles y responsabilidades, así como la dotación de recursos técnicos, humanos y económicos necesarios.

6.4.1.- MEDICIÓN DE RESULTADOS

El análisis de riesgos y el desarrollo de un SGSI o de un Plan de Seguridad son iniciativas costosas y que requieren largos períodos de ejecución, por lo que es necesario proporcionar a la Organización información sobre su evolución y sobre su utilidad.

Los principales objetivos en la elaboración de métricas en el ámbito de la seguridad de la información son:

- Disponer de información actualizada sobre la ejecución de los diferentes proyectos de seguridad a nivel presupuestario y a nivel de tiempos de ejecución.
- Disponer del grado de consecución de los objetivos, en relación con los requerimientos de seguridad planteados.
- Comparar el nivel de seguridad de la Organización con el nivel de otras organizaciones similares, ya sea dentro o fuera del sector o teniendo en cuenta criterios de volumen geográficos, etc., mediante la utilización de comparativas y estudios realizados por entidades independientes.

Las principales tareas a considerar para realizar la medición de los resultados del análisis de riesgos son:

- Definir los objetivos de las mediciones
- Identificar un conjunto reducido de indicadores relevantes que permita dar información precisa sobre los diferentes aspectos a medir.
- Establecer los mecanismos tecnológicos y operativos que permitan realizar el cálculo de los indicadores de forma rápida y precisa.

6.5.- CONCLUSIONES Y RECOMENDACIONES

Primeramente es necesario establecer que para el desarrollo del presente trabajo se tuvieron limitaciones con relación al ámbito real de las instituciones que intervienen en el mercado de valores ecuatoriano, dado a ser un área por su naturaleza altamente confidencial y de información clasificada muy sensible. Motivos por los cuales se hizo muy difícil conocer la realidad de los procesos dentro de la institución, pero de acuerdo a las entrevistas realizadas con personal de la empresa en referencia se pudieron establecer proximidades y de esta manera presentar un caso práctico susceptible a ser analizado y puesto en conocimiento de los altos directivos de la Institución.

Las principales conclusiones obtenidas de la ejecución de este trabajo han sido:

1.- Se ha demostrado claramente la importancia de la función de la Administración de Riesgos de Seguridad asociados a la T.I. dentro de las empresas participantes en el mercado de valores ecuatoriano y de acuerdo a este objetivo alcanzado se propone un modelo que sirva de guía para la

definición e implementación de dicha función basado en objetivos de control y sus actividades correspondientes para crear un medio de seguridad de información.

2.- Se ha analizado, evaluado y diagnosticado la situación actual con respecto a los marcos de referencia y control interno para obtener un sistema que cree un medio ambiente de seguridad de la información que es operada por las Tecnologías de Información. Este punto es imprescindible para asegurar que cualquier ciudadano común y corriente pueda invertir en el mercado de valores ecuatoriano.

3.- Se han identificado los principales activos de información de la Organización en términos de los requerimientos de seguridad definidos, lo que ha permitido identificar las áreas que requieren mayor atención, diferenciándolas de aquellas para las que puede ser suficiente el baseline actual de seguridad.

4.- El apoyo de la Dirección es un factor imprescindible para el éxito del proyecto, debido a la necesidad de contar con la colaboración de personal de diversas áreas de la Organización, en muchos casos de niveles gerenciales o directivos. Adicionalmente, los resultados del análisis de riesgos deben elevarse y someterse a la aprobación de la Dirección que debe conocer los resultados del análisis y las alternativas propuestas para cumplir los requerimientos identificados y formalizados.

5.- La existencia de documentación previa que recoja inventarios, aunque sean parciales de procesos, activos de información, recurso de información, etc. Aumentan significativamente la eficiencia y la calidad de la realización del análisis, ya que permiten realizar un trabajo previo a las entrevistas que las hace más productivas.

6.- Es necesario integrar la información del negocio, que determina lo que es importante y lo que no lo es para el cumplimiento de los objetivos corporativos definidos y la información tecnológica que determina los elementos que es necesario proteger para asegurar un soporte adecuado al cumplimiento de los objetivos de negocio.

7.- Las medidas de seguridad necesarias para proteger la información de la Organización deben ser de diversos tipos: organizativos, tecnológicos, etc. Y trabajar adecuadamente de forma integrada.

8.- Es necesario disponer de un conocimiento profundo tanto de la tecnología como de los procesos de negocio para ejecutar adecuadamente un proyecto de análisis de riesgos que obtenga unos resultados ajustados a la realidad.

9.- La función del analista de riesgos consiste en guiar en el proceso y en aplicarlo con la información proporcionada por el personal de negocio o de tecnología. Se requiere una importante capacidad de comunicación para extraer toda la información necesaria de los participantes sin introducir sesgos ni contaminación.

10.- Dado que uno de los aspectos más importantes del análisis de riesgos en su carácter sistemático, es muy importante la aplicación escrupulosa de la metodología definida de modo que las técnicas, métodos y criterios empleados sean adecuados y homogéneos. Para ello, es importante mantener reuniones de coordinación en las que se traten todos los casos particulares identificados, y que se documenten los criterios seguidos de modo que sean conocidas inequívocamente por parte de todo el equipo.

En conclusiones con referencia al desarrollo del tema en general se puede resaltar los siguientes puntos:

a) La Administración de Riesgos de TI es importante ya que es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

b) La Administración de Riesgos de TI es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario

c) El principal objetivo de la Administración de Riesgos de TI, Como primera ley de la naturaleza, garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos. Muchos de los defectos en la administración de riesgos radica en la ausencia de objetivos claros.

d) Se debe enfatizar y relevar la importancia y significado de la Administración de Riesgos de TI, debido a la trascendencia de los controles y seguridades de los sistemas de procesamiento de información que ameritan ser implementados en toda la organización.

e) La Administración de Riesgos de TI, dentro de la empresa, es una herramienta muy útil para el mejor desarrollo de las actividades de un departamento o de todos los departamentos de la organización.

f) La Administración de Riesgos de Tecnología de Información, nos muestra los principales controles y seguridades que deben implementarse en uno de los departamentos de la empresa como es el caso del departamento de sistemas.

g) El análisis de riesgos de TI, desarrollado en la empresa, ha contribuido al ampliar aún más los conocimientos sobre los problemas significativos que puedan tener el área de sistemas de una empresa y sobre las múltiples ideas de soluciones que se puedan aplicar.

h) En el trabajo se pudieron determinar una serie de hallazgos que son muy importantes en toda empresa como:

- Existencia de Respaldos de las Bases de Datos (Clientes y Proveedores)
- Seguridades de la Información
- Existencia de Bitácoras de las Actividades del Departamento de Sistemas
- Existencia de Planes de Contingencia
- Existencia de seguros para la protección de los Equipos
- Seguridades en la empresa

- Existencia de documentación y de seguridades de la Información
- Existencia de Manuales de Funciones

2. Este trabajo tiene como una de sus metas primordiales el orientar al personal presente y futuro de la empresa, sobre los aspectos importantes que se deben considerar en la administración de riesgos de Tecnología de Información de las empresas del sector bursátil.

3. Este trabajo así como es un apoyo a la empresa, también es una guía para quienes en un futuro desarrollen actividades sobre la Administración de Riesgos de TI en una empresa determinada.

RECOMENDACIONES

1. La empresa del Mercado de Valores ecuatoriano debería designar un área o grupo de personas que se encarguen de implementar los controles determinados en el trabajo en cada departamento, de esta manera es un control integral.

2. El Comité Directivo en conjunto con el departamento de sistemas debería poner énfasis en su organización efectuando los ajustes necesarios y la implementación del Sistema de Administración de Riesgos de Tecnología de Información bajo las directrices de las Normas internacionales y de las mejores prácticas.

3. El Comité Directivo debería contratar al personal debidamente capacitado en el área de Tecnología y de esta manera implantar y mantener líneas de comunicación eficientes, con alto nivel de disponibilidad, que soporten la mejora continua de los procesos y la oportuna atención a los incidentes o riesgos detectados.

4. El Comité Directivo debería fortalecer y actualizar la seguridad de los sistemas y bases de datos, implantando y manteniendo una Tecnología de punta, cuidando de mantener una relación costo-beneficio positive, salvaguardando la continuidad de los negocios en la empresa del Mercado bursátil.

5. Y por último implantar y mantener el Sistema de Administración de Riesgos de Seguridad de la Información integrado, en líneas y un Sistema de Información Gerencial dinámico y confiable. Estableciendo políticas de alto nivel y procesos formales de auto control y autodiagnóstico para el mantenimiento del Sistema incluyendo procesos de culturización hacia todo el personal de la empresa.

6.6. - BIBLIOGRAFÍA

1) AENOR- Asociación Española de Normalización y Certificación, (2011), [En línea] Disponible en: http://www.aenor.es

- Gesttic-Software UNE71501.01, (2001) Tecnología de la Información (TI), Guía para la gestión de la seguridad de TI. (pp.182-210), España
- Gesttic-Software UNE71502. (2009), Tecnología de la Información (TI). Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), (pp.95-110), España.

2) AS/NZS- Australian Standards/ New Zealand Stand,(2010), [En línea] Disponible en ,http://www.standards.com.au/, http://www.standards.com.nz/)

3) Bolívar de Jesús Jumbo (2002),: Revista Financiera, Gestiopolis,, [En línea] disponible en http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/bolsasmundo.htm

4) Bolívar de Jesús Jumbo, (2009), Gestiopolis, La Bolsa de Valores y los principales índices del mundo, , [En línea] Disponible en: http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/bolsasmundo.htm

5) Bolsa Mexicana de Valores, (2010), [En línea] disponible en - www.bmv.com.mx, México D.F.

6) BSI-British Standards Institution,(2010), [En línea] Disponible en: http:--www.bsi-global.com

- BS799-306.3(2006), Information Security Management Systems. Guidelines for Information Security Risk Management.
- [BS25999-1.06] BS 25999-1-2006 Business continuity Management Code of practice.
- [BS25999-2.07] BS25999-2.2007 Business continuity management Specification

7) Cardiff C. Val IT Framework ,(2004) Risk Management Implementation Guide, (pp.32-116)

8) Comité de Supervisión Bancaria Basilea II, (2010), : [En línea] disponible en http://www.bis.org/publ/bcbs189_es.pdf

9) Comparación de modelos de análisis de riesgos:

- University of Glam organ (2004), a critical Discussion of Risk and Threat Analysis Methods and Methodologies S. Vidal's School of Computing. Manuscrito no publicado
- [ENISA06] Inventory of Risk assessment and risk management methods ENISA, 2006.
- COSO- Committee of Sponsoring Organizations of the Tread way Commission , [En línea] Disponible en: www.coso.org
    - [COSO04] COSO, Enterprise Risk Management – Integrated Framework, (2004).
    - OGC-Office of Government Commerce , [En línea] Disponible en: (http://www.ogc.gov.uk)
- [ITIL.06]ITIL V3 Foundation Handbook, Office of Government Commerce,(2009), [En línea] Disponible en: http://www.itilv3.es/
    - [PRINCE06] PRINCE2 Maturity Model, Version 1.0, Office of Government Commerce, 2010, [En línea] Disponible en:http://www.prince-officialsite.com/
- [PM3.06] Portfolio, program me & project management maturity model (P3M3) Version 1.0) Office of Government Commerce, 2006.
- PMI-Project Management Institute, [En línea] Disponible en: (http://www.pmi.org)
- [PMI00] A guide to the Project Management Body of Knowledge (PMBOK Guide), Project Management Institute, 2010.(pp.113-156), USA
- OCDE/ Organización para la cooperación y el Desarrollo Económico 2010. [En línea] Disponible en: http//www.oecd.org/
- [OCDE04] Principios de Gobierno Corporativo, OCDE, 2004.

- ISACA- Information Systems Audit and Control Association, [En línea] Disponible en: http://www.isaca.org
- [ISACA07] Control Objectives for Information and Related Technologies (COBIT) Version 4.1. ITGI. Information Technology Governance Institute, ISACA, (2007), (pp.35-183)

10) CRAMM,(2010), En línea] Disponible en: http://www.cramm.com

- CRAMM03,(2003), CCTA Risk Análisis and Management Method (CRAMM), Version 5.0 CCTA- Central Computing and Telecommunications Agency, (pp.45-79), London

11) Diario de Negocios, Hoy, (2012), [En línea] Disponible en http://www.hoy.com.ec/noticias-ecuador/desde-hoy-las-bolsas-de-guayaquil-y-quito-manejan-un-solo-sistema-529590.html, **Guayaquil**

12) Diccionario de la Real Academia de la Lengua Española,(2010), [En línea] disponible en http://www.rae.es/rae.html

13) Dr. Cancelado G. Alberto, (2010), Buenas tareas Ensayos, Sistemas de Administración de Riesgos en Tecnología Informática. [En línea] disponible en http://www.buenastareas.com/ensayos/Sistemas-De-Administracion-De-Riesgos-En/581327.html

14) Dr., Filorio Tenorio Ramón, Director del área de Tecnología de Información, Indeval S.A., (2010), México D.F.

15) Dr. Julio Clavijo Acosta, (2010) , Fundación Ecuador Libre, [En línea] disponible en: http://www.ecuadorlibre.com/index.php?option=com_content&view=article&id=415:cap-no163-qel-mercado-de-valores-ecuatorianoq&catid=3:capsula-de-entorno-economico&Itemid=12

16) Dr. Navarrete C. Roberto, (2010), Revista Financiera Gestiopolis, [En línea] disponible en: http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/usoti.htm

17) Dr. Rosario Jimmy, (2010), Observatorio para la Cibersociedad, [En línea] disponible en http://www.cibersociedad.net/archivo/articulo.php?art=218

18) Econ. Luis Rosero M, (2009), [En línea] Disponible en: www.bce.fin.ec/documentos/PublicacionesNotas/.../BPrensa149.pdf., Guayaquil

19) FAIR- Factor Analysis of Information Risk, [En línea] Disponible en: (www.riskmanagemtinsight.com)

20) F.López M.A: Amutio J. Candau y J.A. Mañas. Ministerio de Administraciones Públicas, (2006), Metodología .de Análisis y Gestión de Riesgos de los Sistemas de Información versión 2.

21) IEEE Section México, The Institute of electrical and electronics engineers Inc., (2010), [En línea] disponible en http://www.ieee.org.mx/IEEE/IEEE_Seccion_Mexico.html

22) Indeval, (2010), [En línea] disponible en: www.indeval.com.mx, México D.F.

23) Inteco Cert, (2006), Instituto Nacional de Tecnologías de la Comunicación. [En línea] disponible: www.cert.inteco.es

24) ISACA, Information Systems Audit and Control Association, Risk IT Framework, (2010), (pp.5 al 50)

25) ISO – International Standards Office , 2010, [En línea] Disponible en: http//www.iso.org

- [ISO13335-1.04] ISO/IEC TR 13335-1, 2004, Information technology-Security techniques-Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security Management.

- [ISO27005.08] ISO/IEC 27005-2008, Tecnología de la Información. Técnicas de seguridad, Gestión de riesgos de Seguridad de la información.
- [ISO 20000-2.05] ISO/IEC 20000-2, (2005), Tecnología de la información-Gestión del servicio- Código de buenas prácticas.
- [ISO 31000-2009] ,Tecnología de la Información-Gestión de los riesgos de Seguridad de la Información

26) J. Jones Risk Management Insight, (2005). [JONES05A] An introduction to Factor Analysis of Information Risk (FAIR). A framework for understanding, analyzing, and measuring information risk. (pp.38-65),EE.UU

- J. Jones Risk Management Insight, (2008), [JONES08B]Risk Evolution Part II

27) Julio Baldeón,(1998), Monografías, [En línea] disponible en http://www.monografias.com/trabajos13/desamerc/desamerc.shtml, Guayaquil

28) MAGERIT, (2006), [En línea] Disponible en: http://publicaciones,administracion.es

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

29) Mary Walton, W. Edwards Deming, Bogotá, (2004), Traducción Margarita Cárdenas - Grupo Editorial Norma - El método Deming en la práctica / (pp.46-132) Bogotá,

30) Mtro. Carlos Zamora, (2011), Consultoría Estratégica Conseti S.A., México D.F., Manuscrito no publicado (entrevista)

31) Mtro. Jorge Garibay, Redit S.A., entrevista e información ,(2011), México D.F., Manuscrito no publicado

32) NIST-National Institute of Standards and Technology,), [En línea] Disponible en: http:www.nist.gov

- G. Stone burner A. Goguen y A. Feringa, NIST Special Publication, (2002). [NIST800-30.02] NIST SP 800-30, Risk Management Guide for Information Technology Systems (pp.46-134), EE.UU
- R. Ross S .Katzake, A. Johnson Swanson G. Stone burner y G. Rogers, NIST Special Publication. 2004. [NIST800-53.04]NIST SP 800-53 Recommended Security Control for Federal Information Systems

33) OEM, Organización Editorial Mexicana, (2008), [En línea] disponible en http://www.oem.com.mx/esto/notas/n911892.htm, México D.F.

34) OCTAVE, (2010), [En línea] Disponible en: http://www.cert.org/octave

- Albert y A. Doro fee Carnegie Mellon University, (2001), ALBER01 OCTAVE Method Implementation Guide Version 2.0.C. (pp.75-110), EE.UU.
- Albert y A. Doro fee, Addison Wesley, (2003), ALBER03A, Managing information Security Risks. The Octave Approach, C. (pp.64-121),EE.UU
- Albert, A. Doro fee J. Stevens C. Woody, Carnegie Mellon University, (2005).

- R. Caralli Stevens, Young Wilson. Carnegie Mellon University, 2007, ALBER05, OCTAVE-S Implementation Guide, Version 1.0 [ALBER07] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

35) Osiatis,(2006), [En línea] disponible: en: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/vision_general_gestion_servicios_TI/vision_general_gestion_servicios_TI.php

36) Osiatis,(2010), ITIL- Gestión de Servicios TI,), [En línea] disponible en http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servi

cio/proceso_gestion_de_la_continuidad_del_servicio/organizacion_y_planificacion_de_la_continuidad_del_servicio.php

37) PWC, 2006, PricewaterhouseCoopers (Ed), (2006), Manual de Curso GO SPA , México D.F. Manuscrito no publicado

38) SOMAP – Security Officers Management & Análisis Project [En línea] Disponible en: (http://www.somap.org/)

- [SOMAP07} Open Information Security Risk Assessment Guide, Version 1.0 SOMAP org. 2007

39) Superintendencia de Compañías del Ecuador,(2010), [En línea] disponible en http://www.supercias.gov.ec/Documentacion/Mercado%20Valores/Marco%20Legal/Ley%20Mercado/Ley%20MV.pdf

40) Wikipedia, Enciclopedia libre, (2010), : [En línea] disponible en http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

ANEXOS

ANEXO 1

BASILEA II

Basilea II, estándar internacional que sirve de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

El denominado acuerdo de capital, más conocido como Basilea II, pretende que las entidades financieras aprovisionen las pérdidas por impago en función de la calidad crediticia de su cartera de clientes de activo (hipotecas, préstamos personales, etc.). Para ello, estas compañías deberán disponer de modelos automáticos de decisión que anticipen el comportamiento de los clientes y cuantifiquen esa posible pérdida, permitiendo a las entidades medir la rentabilidad de su cartera de clientes de forma más adecuada. De esta manera podrán ofrecer un tratamiento más individualizado y aplicar una política de precios que asegure la cobertura de pérdidas y posibilite la discriminación, premiando a los buenos clientes y penalizando a los malos.

Basilea II describe al riesgo operativo como, el riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

GRÁFICA NO.20 CUADRO EXPLICATIVO DEL RIESGO DE ACUERDO A LA NORMA INTERNACIONAL BASILEA II

Basilea presenta tres métodos para calcular los requerimientos de capital por riesgo operacional, en orden creciente de sofisticación y sensibilidad al riesgo, siendo éstos:

- El método del indicador básico
- El método estándar
- Los métodos de medición avanzada (AMA)

- **El método del indicador básico.**- Las instituciones que participen en el mercado de valores ecuatoriano deberán cubrir el riesgo operacional con un capital equivalente al promedio de los tres últimos años de un porcentaje fijo (denotado como alfa) de sus ingresos brutos anuales positivos.
- **El método estándar.-** En este método las actividades de las instituciones financieras se dividen en ocho líneas de negocio:

  1.- Finanzas corporativas
  2.- Negociación y ventas
  3.- Banca Minorista
  4.- Banca Comercial
  5.- Pagos y liquidación
  6.- Servicios de agencia
  7.- Administración de activos
  8.- Intermediación minorista

El ingreso bruto de cada línea de negocio es un indicador amplio que permite aproximar el volumen de operaciones del banco y, con ello, el nivel del riesgo operacional que es probable que asuma el banco en estas líneas de negocio.

- **Métodos de Medición Avanzada (AMA)**

Al objeto de poder utilizar los AMA, el banco deberá demostrar a su supervisor que, como mínimo:

- Su consejo de Administración y su Alta Dirección, según corresponda, participen activamente en la vigilancia del marco de gestión del riesgo operacional.
- Posee un sistema de gestión del riesgo operacional conceptualmente sólido que aplica con integridad.
- Cuenta con recursos suficientes para utilizar la metodología en las principales líneas de negocio, así como en los ámbitos de control y auditoría.

Está conformado por: Criterios cualitativos y cuantitativos.

Basilea establece que estos modelos desarrollados deberán ser implementados por sistemas software de inteligencia de negocio que ayuden en la mejora de dicha administración del riesgo. Uno de los puntos críticos para cumplir con la normativa Basilea II tiene que ver con la forma de administrar la información. Para optimizar los procesos de control del riesgo y elaborar modelos altamente predictivos no sólo es importante contar con un volumen de datos histórico-significativos, sino poder integrar todo el proceso de gestión de dicha información.

Una adecuada integración tecnológica supone incorporar a los procesos y sistemas de gestión del riesgo toda la información disponible que interviene, influye o condiciona, de alguna forma, la toma de decisión más acertada para resolver las operaciones de crédito. Pero además, para optimizar los procesos, los distintos accesos deben realizarse de forma automática, siguiendo los workflows previamente definidos por la dirección de riesgos de la entidad, según su modelo predictivo.

ANEXO 2

ESCALA DE VALORACIÓN DE REQUERIMIENTOS DE SEGURIDAD

Criterios de valoración		Valor				
		Crítico (10)	Alto (5)	Medio (2)	Bajo (1)	Nulo (0)
Estrategia de la Organización		Imposibilidad de seguir la estrategia fijada	Impacto grave sobre la estrategia	Impacto moderado sobre la estrategia	Impacto leve sobre la estrategia	No afecta a la estrategia de la Organización
Operaciones	Daños personales	Pérdida de varias vidas	Pérdida de una vida	Lesiones graves a una o varias personas	Daños leves a una o varias personas	No afecta a la seguridad de las personas
	Orden público	Alteración seria del orden público	Manifestaciones o presiones significativas	Protestas puntuales	Generación de malestar	No afecta al orden público
	Actividad de la Organización	Interrupción permanente de las actividades	Interrupción prolongada de las actividades	Interrupción breve de las actividades	Entorpecimiento de las actividades	No afecta a la actividad de la Organización
	Intereses comerciales (valor comercial)	Interés muy grande para la competencia	Alto interés para la competencia	Interés moderado para la competencia	Bajo interés para la competencia	Sin interés para la competencia
	Impacto sobre terceros (clientes, proveedores) (Evaluar la gravedad mediante los otros criterios)	Grave impacto para muchos terceros	Grave impacto para pocos terceros. Impacto moderado para muchos terceros	Grave impacto para un tercero. Impacto moderado para pocos terceros. Impacto leve para muchos terceros.	Impacto moderado para un tercero. Impacto leve para pocos terceros.	Impacto leve para un tercero. Sin impacto para terceros
	Relaciones internacionales	Impacto en las relaciones internacionales a alto nivel	Impacto en las relaciones internacionales a nivel diplomático	Impacto en las relaciones internacionales	Impacto leve en las relaciones internacionales	No tiene impacto en las relaciones internacionales
Información financiera y de gestión		Deficiencias materiales en la información	Deficiencias significativas en la información	Deficiencias moderadas en la información	Deficiencias leves en la información	Sin impacto sobre la información
Cumplimiento	Obligaciones legales y reglamentarias	Incumplimiento excepcionalmente grave de la ley	Incumplimiento grave de la ley	Incumplimiento moderado de la ley	Incumplimiento leve de la ley	Sin impacto sobre el cumplimiento
	Obligaciones contractuales	Incumplimiento excepcionalmente grave de obligaciones contractuales. Posible cancelación de contratos relevantes.	Incumplimiento grave de obligaciones contractuales. Posibilidad de incurrir en penalizaciones relevantes.	Incumplimiento moderado de obligaciones contractuales. Posibilidad de deterioro de las relaciones con terceros relevantes.	Incumplimiento leve de obligaciones contractuales.	Sin impacto sobre el cumplimiento

ANEXO 3

DESCRIPCIÓN DE IMPACTOS AL NEGOCIO DEL MERCADO DE VALORES ECUATORIANO

1.- AMBIENTE

- Competencia.- Riesgo de Pérdida de ventaja competitiva en el entorno del negocio de la organización, debido a la falta de provisión de productos y servicios que satisfagan a los clientes, afectación de la calidad, costos no competitivos, tiempos de respuesta superiores a los de la competencia.

- Sensibilidad.- Cuando se comprometen los recursos de la compañía y flujos de efectivo esperados en el futuro, en tal extensión que reduce la tolerancia de la compañía a los cambios del ambiente que se encuentran totalmente fuera de su control, por ejemplo: cambios en tasas de interés, tipos de cambio de monedas extranjeras, inflación, tratados internacionales y otras condiciones económicas.
  Este riesgo también se presenta cuando la organización es muy inflexible a cambiar en respuesta a cambios en el ambiente.

- Relaciones con los accionistas.- Degradación en la confianza que tienen los inversionistas, los mismos que no tienen la suficiente confianza de que la organización tiene el potencial para proveer un retorno de la inversión suficiente.

- Disponibilidad de capital.- La compañía no tiene el accesos suficiente al capital que requiere para operar, ejecutar sus estrategias y generar futuros retornos financieros.

- Pérdidas por catástrofes.- La incapacidad para mantener las operaciones, proveer los productos y servicios esenciales o recuperar los costos operativos como resultado de un desastre mayor. La inhabilidad para recuperarse en caso de desastres puede dañar la reputación de la organización, su habilidad para obtener capital y afectar su relación con inversionistas.

- Soberanía/ Político.- El riesgo de consecuencias adversas derivadas de acciones políticas en el país en donde la organización realiza inversiones significativas, depende su negocio en un porcentaje alto o ha realizado acuerdos con una contraparte sujeta a las leyes de ese país en particular. Por ejemplo posible nacionalización o expropiación de activos sin compensación.

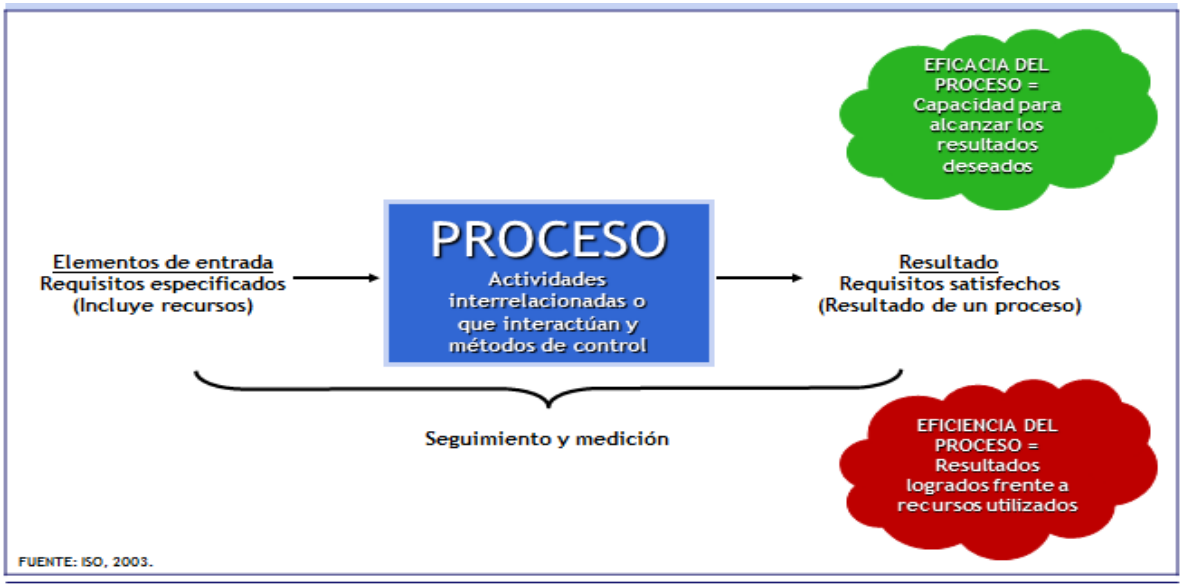
- Legal.- El riesgo de que las transacciones de la organización, acuerdos contractuales, estrategias específicas y actividades contravengan con las leyes aplicables en el país.

- Regulaciones.- El riesgo de no cumplir con regulaciones emitidas por entidades reguladoras internacionales, nacionales y locales.

- Industria.- El riesgo de que la industria, en este caso el mercado bursátil, pierda su atractivo, debido a cambios en factores clave para el éxito competitivo de la organización dentro de la industria. En general, cualquier impacto adverso al funcionamiento del mercado bursátil.

- Mercados financieros.- Impacto en el desempeño y control del mercado financiero. Exposición a cambios en las variables del mercado.

2.- PROCESOS



Operaciones.- Dentro de este grupo se puede citar por ejemplo: accesos no autorizados, fraude de empleados, sistema obsoleto, ausencia de gestión experta, riesgo del proveedor del servicio de red, cliente no cumple las políticas de seguridad, cliente niega haber realizado una transacción, entre otras.

Pero subdividiendo este rubro lo podríamos clasificar en:

- Satisfacción del cliente.- El riesgo de que los procesos de la organización no cumplan o excedan de manera consistente las expectativas de los clientes. Clientes insatisfechos.

- Recursos humanos.- Pérdida del conocimiento, habilidades y experiencias necesarios para asegurar que los objetivos críticos de la organización son alcanzados.

- Desarrollo de producto.- Impacto en el proceso de desarrollo de productos y servicios.

- Eficiencia.- Impacto en la capacidad de la organización para ejecutar sus procesos de manera eficiente.

- Capacidad.- Incapacidad para operar los procesos críticos del negocio de acuerdo con los niveles de servicio esperados y/o desarrollar servicios de acuerdo con la capacidad instalada.

- Brechas de desempeño.- Impacto en los procesos del negocio que le impide a la organización operar de acuerdo con las mejores prácticas de la industria. Está relacionado con disminución de la calidad, costos más altos, tiempos de ciclo más largos.

- Tiempo de ciclo.- Impacto en el tiempo esperado para el inicio y terminación de un proceso del negocio (o actividad dentro del proceso). El tiempo puede alargarse debido a redundancia, realizar pasos innecesarios o repetitivos.

- Abastecimiento.- Impacto en la disponibilidad de la información para la operación de la organización, incluyendo energía.

- Obsolescencia.- Faltante.- El riesgo de que los activos necesarios para ejecutar el proceso del negocio sean excesivos, se encuentren obsoletos o fallen.

- Cumplimiento.- Falta de cumplimiento de las especificaciones de los clientes, políticas y procedimientos organizacionales e incluso leyes y regulaciones internacionales, nacionales y locales.

- Interrupción del negocio.- Falta de los materiales, recursos humanos con la experiencia, conocimiento y habilidades requeridas, tecnología de información y otros recursos que provocan una interrupción en la operación de los procesos críticos de la organización.

- Defectos en el servicio.- Impacto en el servicio prestado por la organización derivando en defectos.

- Ambientales.- Relacionados con impacto al medio ambiente, incluyendo contaminación, derrames, explosiones.

- Salud y Seguridad.- Impactos en la salud y seguridad del personal de la organización.

- Marca/Desgaste de la marca.- Impacto en el valor de la marca o imagen de la organización.

3. - EMPODERAMIENTO

- Liderazgo.- Falta de los recursos humanos necesarios para proveer del liderazgo, visión y soporte necesario para ayudar a los empleados a ejecutar de manera efectiva sus actividades y cumplir con sus responsabilidades.

- Autoridad/Límites.- El riesgo de que una persona o grupo de personas tomen decisiones y/o realicen acciones que no se encuentran dentro de su responsabilidad explícita, o bien, que no tomen la responsabilidad que les corresponde.

- Outsourcing.- El riesgo de que proveedores externos no realicen las actividades que les corresponden dentro de sus responsabilidades o bien que el proveedor de procesos estratégicos para el negocio se convierta en competidor.

- Incentivos de desempeño.- Ocurre cuando los gerentes y empleados son monitoreados utilizando medidores de desempeño que los obligan a actuar de una manera que es inconsistente con los objetivos, estrategias, estándares éticos y prácticas de la organización.

- Disposición al cambio.- Las personas dentro de la organización no pueden implementar/ ejecutar los procesos del negocio con la suficiente rapidez que requiere los cambios en el entorno de la organización.

- Comunicaciones.- Impacto en las comunicaciones entre el personal.

4. - TECNOLOGÍAS DE INFORMACIÓN (TI)

- Importancia/Relevancia.- Riesgo de que la información no sea relevante para los propósitos por los cuales fue recolectada, almacenada o distribuida.

- Integridad.- Todos los riesgos asociados con la autorización y con las propiedades que la información sea exacta y esté completa.

- Acceso.- El riesgo de que personas no autorizadas tengan acceso a información sensible o confidencial, o bien, que personas autorizadas no puedan acceder a la información para la cual se encuentran autorizados.

- Disponibilidad.- El riesgo de que la información no se encuentre disponible cuando se requiere.

- Infraestructura.- El riesgo de no contar con la infraestructura adecuada. Dentro de este rubro podemos considerar el desarrollo de software cuyos riesgos más importantes son:

  Cronograma de la etapa de construcción de software mal definido, Incumplimiento del proveedor de Outsourcing, Retiro de la compañía del proveedor de pruebas, daño del servidor de desarrollo, nuevas vinculaciones de analistas (arquitectos del proyecto). Cambio de Gerente del proyecto, Mal definido los requisitos funcionales por parte del usuario final, mala definición funcional de guión de pruebas, Solicitud de nuevos desarrollos en la etapa de prueba.

5.-INTEGRIDAD

- Fraude de la gerencia.- Emisión de declaraciones financieras manipuladas y en general el uso indebido de recursos financieros de la organización.

- Fraude de los empleados.- El riesgo de que los empleados, clientes o proveedores ya sea de manera individual o conjunta cometan actos fraudulentos contra la organización, resultando en pérdidas financieras o uso no autorizado de activos físicos, financieros o de información.

- Actuaciones ilegales.- Gerentes y empleados en lo individual o de manera coludida comentan actos ilegales que pueden tener consecuencias para la organización.

- Usos no autorizados.- El riesgo de que empleados y /u otras personas hagan uso de activos físicos, financieros y/o información de manera no autorizada y/o ética.

- Reputación.- El riesgo de que la organización vea afectada su reputación, pudiendo perder clientes, empleados clave o su habilidad para competir, debido a la percepción de que la organización no actúa de manera honesta ante sus clientes, proveedores y accionistas o no administra correctamente el negocio. La pérdida de clientes implica la pérdida de ingresos, la pérdida de personal clave que implica pérdida de talento, habilidades y experiencia, la pérdida de proveedores significa la pérdida de materiales y sistemas para ejecutar los procesos del negocio y la pérdida de habilidad para competir significa eventualmente, el cierre del negocio.

6. - PRECIO

- Tasa de interés.- Riesgo de que las tasas de interés se desvíen de los valores esperados.

- Moneda.- Exposición a fluctuaciones en tipos de cambio de monedas

- Patrimonio.- Exposición a las fluctuaciones en el flujo de ingresos derivados de inversiones en acciones públicas, inversiones en entidades privadas, ofertas de acciones, etc.

- Commodity.- Exposición a fluctuaciones de precio en sistemas de tecnología.

- Instrumentos financieros.- Riesgos relacionados con impactos en instrumentos financieros.

7. - LIQUIDEZ

- Flujo de efectivo.- Pérdidas resultantes de la imposibilidad de fondear obligaciones operacionales o financieras de la organización.

- Costos de oportunidad.- Costos derivados de la falta de oportunidad en la ejecución de los procesos de la organización.

- Concentración.- Pérdidas resultantes de la inhabilidad de acceder al efectivo en forma oportuna.

8. - CRÉDITO

- Incumplimiento.- Imposibilidad de cumplir con obligaciones relativas a créditos.

- Concentración.- Exposición a pérdidas excesivas por concentración de crédito en grandes volúmenes a clientes, industria u otro segmento económico en particular.

- Cancelación.- Riesgos relacionados con la cancelación de créditos.

- Garantía.- Pérdidas parciales o totales de garantías.

ANEXO 4

INFORMACIÓN PARA LA TOMA DE DECISIONES

OPERACIONAL.-

- Fijación de precios.- Impactos relacionados con la fijación de precios en forma inadecuada.

- Establecer compromisos.- No contar con la información necesaria para dar seguimiento a compromisos contractuales.

- Medición del desempeño.- Información de medidores de desempeño errónea y/o que no refleje la realidad.

- Alineación.- El riesgo de que los objetivos y medidores de desempeño de los procesos de la organización no se encuentren alineados con los objetivos generales y estrategias de la organización.

- Informes obligatorios. El riesgo de que los reportes operativos requeridos por agencias reguladoras estén incompletos, inexactos, fuera de tiempo y que expongan a la compañía a multas, penalizaciones y sanciones.

FINANCIERAS

- Presupuesto y planificación.- No contar con la información necesaria para el proceso de planificación y desarrollo del presupuesto.

- Información contable.- Riesgo de no contar con información contable relevante, integra y confiable.

- Evaluación de informes financieros.- El riesgo de no contar con la información necesaria para el desarrollo de los informes financieros que sea relevante, íntegra y confiable.

- Impuestos.- No contar con la información relativa a impuestos que sea relevante, íntegra y confiable.

- Fondos de pensiones.- No contar con la información relativa a fondos de pensiones.

- Análisis de inversiones.- Falta de información para tomar decisiones respecto a inversiones a corto, mediano y largo plazo.

- Informes obligatorios.- El riesgo de que los reportes financieros requeridos por agencias reguladoras estén incompletos, inexactos, fuera de tiempo y que expongan a la organización a multas, penalizaciones y sanciones.

ESTRATÉGICAS

- Análisis del entorno.- El riesgo de no contar con la información relativa al entorno externo (ambiente), que permita identificar y analizar cambios y ejecutar las estrategias necesarias.

- Cartera del negocio.- El riesgo de no contar con la información relativa al portafolio de la organización-

- Valoración.- No contar con la información necesaria para valorar el negocio actual y nuevas oportunidades de negocio.

- Medición del desempeño.- Información de medidores de desempeño erróneas y/o que no reflejen la realidad.

- Estructura de la organización.- No contar con la información relacionada con la estructura organizacional que sea relevante, integra y confiable.

- Asignación de recursos.- No se cuenta con la información relacionada con la asignación de recursos que permita maximizar la ventaja competitiva y retornos para accionistas.

- Planificación.- No contar con la información relativa a la planeación de estrategias de negocio que sea relevante, íntegra y confiable.

- Ciclo de vida.- No contar con la información relativa al enfoque de la organización para administrar sus líneas de productos y servicios de acuerdo con la evolución de la industria.

ANEXO 5

ENTREVISTAS APLICADAS

CUESTIONARIO 1.

Preguntas de la entrevista que se deberá realizar para obtener la información acerca de los sistemas

1.- ¿Cuáles son los sistemas que se considera más importantes para la empresa? ¿Qué tan bien satisfacen los requerimientos de la misma?

2.- En general, los sistemas del cliente ¿han sido desarrollados internamente o son paquetes estándar? En el caso de paquetes, ¿Qué nivel de adaptación se ha hecho? ¿Quién realiza los cambios (el proveedor o la empresa)?

3.- ¿Cuán antiguos son los sistemas? ¿Requerirán cambios relevantes en el futuro cercano?

4.- ¿Cuáles son las principales locaciones de procesamiento? ¿Cuáles son los principales ambientes de hardware y software de base?

5.- ¿Son confiables los sistemas? ¿Proveen información íntegra, exacta y útil para la gestión y control del negocio?

6.- ¿Cómo están conectados los diversos ambientes TI? ¿Cuáles son las conexiones principales con redes externas? Por ejemplo: EDI, EFT e Internet)

7.- ¿Se utilizan proveedores externos de servicios (Outsourcing)? Si es así que actividades y componentes han sido tercerizados. ¿Cuáles son los contactos clave?

8.- ¿Está cualquier parte de la infraestructura de TI de la compañía compartida o conectada con la estructura de TI de una compañía relacionada o no relacionada?.

9.- ¿Existen aplicaciones de E-business en uso?

Si es así:

- ✓ Identificar partes de terceros más significativas que están conectadas a los sistemas de la empresa. ¿Cuáles son sus principales roles y qué nivel de accesos tienen a los sistemas de la compañía?
- ✓ ¿Qué mecanismos de seguridad se han establecido, tales como firewalls?
- ✓ ¿Han existido incidentes de seguridad relacionados con E-business, por ejemplo, hackeo en el sitio web?

CUESTIONARIO 2

Preguntas de la entrevista que se realizará para obtener la información acerca de la organización del personal

1.- ¿Cuál es la estructura organizativa de TI?

2.- ¿Cuál es el nivel de dependencia respecto al personal superior?

3.- ¿Está el número y experiencia del staff de TI alineado con las necesidades de la operación?

4.- ¿Están claramente definidos los roles y responsabilidades de TI?

5.- ¿Se han producido cambios significativos en la estructura organizativa de TI durante el ejercicio?

6.- ¿Quién es el responsable máximo de TI? ¿A quién le reporta?

7.- ¿Existe un Comité de TI? ¿Cómo se determinan y alinean las prioridades de TI con la estrategia y prioridades del negocio?

8.- ¿Quiénes son los contactos claves en el departamento de TI?

9.- ¿Existen actividades informáticas significativas fuera de la función de TI?

10.- ¿En caso operativo tienen las personas que administran dichas actividades los conocimientos y experiencia apropiados?

11.- ¿Se tienen establecidos programas adecuados de entrenamiento?

12.- ¿Existe una adecuada segregación de tareas dentro de la función de TI?

CUESTIONARIO 3

Preguntas para descubrir los problemas de TI

1.- ¿Está claro lo que está haciendo?

2.- ¿Con qué frecuencia los proyectos de TI no cumplen lo que prometieron?

3.- ¿Son los usuarios finales satisfechos con la calidad de los servicios de TI?

4.- ¿Son suficientes los recursos de TI y la infraestructura disponible para satisfacer los objetivos estratégicos de la empresa?

5.- ¿Son las competencias básicas de TI mantenerse a un nivel suficiente para satisfacer los objetivos estratégicos?

6.- ¿Cuál ha sido la saturación media de los presupuestos de funcionamiento?

7.- ¿Con qué frecuencia y cuántos proyectos van por encima del presupuesto?

8.- ¿Cuánto tiempo se tarda en hacer grandes decisiones de TI?

9.- ¿Son el esfuerzo total de las inversiones y son transparentes?

10.- ¿Cuál es el porcentaje de ingresos (puede ser reemplazado por el presupuesto para el sector público) invertido en TI en comparación con la media del sector?

11.- ¿Cómo ha evolucionado a lo largo de los años?

12.- ¿Cuál es la cantidad que se gasta en TI en comparación con el de la empresa ganancia total (ganancia puede ser sustituido por el presupuesto para el sector público)?

13.- ¿Es compatible con la empresa TI en el cumplimiento de los reglamentos y los niveles de servicio?

CUESTIONARIO 4

Preguntas que debe hacer para averiguar la Gestión de Riesgos de Seguridad de Tecnologías de Información

1.- ¿Cuál es la importancia que la empresa le asigna al mantenimiento de la infraestructura de TI?

2.- ¿Qué iniciativas estratégicas ha iniciado la dirección ejecutiva con relación a la Gestión de riesgos de seguridad de TI y la criticidad en relación con el crecimiento de la empresa?

3.- ¿Qué está haciendo la organización en aprovechar los conocimientos para aumento de valor para los accionistas?

4.- ¿Qué activos de TI existen y cómo se manejan?

5.- ¿Está la empresa clara en su posición relativa a la tecnología. En qué nivel se clasificaría: pioneros, seguidor o rezagados?

6.- Dentro de la participación general de la empresa ¿qué lugar ocupa TI dentro del establecimiento de la dirección estratégica?

7.- ¿La empresa fomenta y apoya la cultura de cambio hacia procesos y perspectivas de negocio que establezcan un crecimiento futuro para la organización?

8.- Es la empresa clara en su posición relativa a los riesgos: evita riesgos o toma riesgos?

9.- Existe en la empresa un inventario actualizado de los riesgos relevantes para la empresa?

10.- ¿Qué se ha hecho como organización para hacer frente a los riesgos?

11.- ¿Hasta dónde debe ir la empresa en la mitigación del riesgo y el costo justificarse por el beneficio?

12.- ¿Qué está haciendo la gestión de riesgos actual de la empresa para hacer frente a los mismos?

13.- ¿Es la Junta periódicamente informada sobre los riesgos a los que la empresa está expuesto?

14.- ¿En base a estas preguntas, la empresa puede decidirse a tomar precauciones razonables en relación a los riesgos de la tecnología?

15.- ¿Qué está haciendo la organización frente al valor del riesgo y manejo de los recursos?

16.- ¿Cuál considera que es la mejor práctica en la administración de riesgos y cómo se compra la empresa con respecto al valor, riesgo y manejo de los recursos?

CUESTIONARIO 5

Preguntas de autoevaluación de Gobierno de TI con relación a la Administración de Riesgos de Seguridad de la Información

1.- ¿Es consciente la Junta Directiva de los últimos avances en TI y sus respectivos riesgos de seguridad de la información desde el punto de vista de una empresa en perspectiva?

2.- ¿Es un tema permanente del orden del día y va dirigido de una manera estructurada?

3.- ¿La Junta Directiva tiene un punto de vista sobre cómo y cuánto la empresa invierte en TI, los riesgos inherentes y la perspectiva de cambio en comparación con otras organizaciones?

4.- ¿El Consejo de TI obtiene informes de rendimiento que ilustre el valor de las TI desde la perspectiva del conductor de negocios (servicio al cliente, costos, agilidad, calidad, etc.)?

5.- Es la Junta Directiva regularmente informada sobre los riesgos de TI a los que está expuesta la empresa incluyendo los riesgos de cumplimiento?

6.- La empresa dispone de un tablero de seguridad estableciendo los recursos de TI adecuados, la infraestructura y las habilidades disponibles (incluidos los recursos externos) para cumplir con los objetivos estratégicos de la organización?

7.- Con relación a los controles de los riesgos identificados de seguridad de información ¿cómo están realizando la gestión del mismo en la actualidad?

GLOSARIO

GLOSARIO DE TÉRMINOS

En este glosario se presentan los términos de uso frecuente en el entorno del análisis de riesgos. Junto a la definición de cada término se ha introducido la traducción al inglés, para facilitar la comprensión de la literatura técnica escrita en ese idioma.

En la elaboración de este glosario se han tenido en cuenta las definiciones recogidas en los principales estándares que se detallan en el apartado de Estado de la Cuestión. Para cada término se ha seleccionado el que se ha considerado más adecuado en el contexto del proyecto, y en algunas entradas se ha preparado una nueva definición que se ha considerado más apropiada para este entorno.

Aceptación (Aceptation): Estrategia de gestión de riesgos que consiste en la aceptación del nivel de riesgo actual. Puede seleccionarse automáticamente si el nivel de riesgo es inferior al umbral de riesgo considerando tolerable o tras un análisis coste/beneficio considerando las alternativas disponibles para reducir o eliminar un riesgo superior.

Actividades de control.- Las actividades de control son las políticas y procedimientos que ayudan a asegurar que la respuesta a los riesgos correctamente efectuada. Las actividades de control ocurren en todos los niveles y funciones de la organización. [Santillana, 2003]

Activo (Asset): Cualquier elemento valioso o necesario para la Organización cumpla sus objetivos. Cfr. [ISO 13335-1.04], Cfr. [ALBER01]

Activo de información (Information Asset): Cualquier información valiosa o necesaria para que la Organización cumpla sus objetivos.

Acuerdo de nivel de servicio (Service level agreement): Acuerdo entre dos partes en relación a las características mínimas exigibles a un servicio prestado entre ellas.

Administración: La palabra ¨Administración¨ se forma del prefijo ¨ad¨, que significa hacia y de ¨ministratio, que viene a su vez de ¨minister, vocablo compuesto de ¨minus, comparativo de inferioridad y del sufijo ¨ter, que sirve como término de comparación. Conjunto de técnicas sistemáticas que permite que las organizaciones sociales logren sus fines. Acción de planear, controlar y dirigir los recursos de una organización con el fin de lograr los objetivos deseados. [Hernández, Ballesteros, 1990]

Adquirir e Implementar (AI).- Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificados, desarrolladas o adquiridas así como la implementación e integración 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. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia. ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?, ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?, ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?, ¿Los cambios afectarán las operaciones actuales del negocio? [COBIT, 2005]

Amenaza (Threat): Causa potencial de un incidente que puede resultar en un daño a un sistema o a una organización [ISO13335-1.04], [ISO27002.05]

Análisis cualitativo (Qualitative analysis): Análisis basado en el uso de escalas de valoración Cfr. [ISO13335-1.04]

Análisis cuantitativo (Quantitative analysis): Análisis basado en cuantificación numérica de magnitudes, generalmente en términos económicos. Cfr. [ISO13335-1.04]

Análisis de impacto sobre el negocio (Impact analysis): Estudio de las consecuencias que tendría la realización de una determinada amenaza sobre la Organización. Cfr. [MAGE06]

Análisis de riesgos (Risk analysis, Risk assessment): Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización [MAGE06], Cfr. [ISO13335-1.04]

Análisis mixto (Mixed analysis): Análisis que emplea una combinación de términos cuantitativos y cualitativos. Cfr. [ISO13335-1.04]

Apetito de riesgo (Risk apetite): Cantidad de riesgo que una Organización está dispuesta a gestionar para lograr los objetivos establecidos.

Ataque (Attack): Amenaza de origen intencionado. Cfr. [MAGE06]

Ataque de día cero (Zero Day Attack): Ataque que se produce antes de la publicación de la vulnerabilidad que explota.

Autenticidad (Authenticity): Propiedad que asegura que la identidad de un elemento o recurso es la que se le supone. La autenticidad aplica a elementos como usuarios, procesos, sistemas e información [ISO13335-1.04]

Brechas de operación: Son aquellos lugares o situaciones en donde las operaciones reales fallan en dar los resultados esperados.

Ciclo de Deming (PDCA cycle): Ver ciclo de la mejora continua.

Ciclo de la mejora continua (PDCA cycle): Herramienta de gestión para la evolución de los procesos que define cuatro fases (planificación, ejecución, comprobación, actuación).

Concienciación (Awareness): Conjunto de medidas definidas para que las personas relacionadas con la organización (personal, personal subcontratado, clientes, proveedores, etc.) conozcan los riesgos de seguridad y los controles que pueden y deben aplicar para colaborar en su mitigación.

Confidencialidad (Confidentiality): Propiedad de que la información no está disponible ni es divulgada a personas, procesos o dispositivos no autorizados. [ISO13335-1.04], Cfr. [ISO27002.05], Cfr. [MAGE06], Cfr. [ALBER01]

Control (Control): Ver salvaguarda.- Cualquier medida que tome la dirección, el consejo y otros, para mejorar la gestión de riesgo y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección, planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas. [Santillana, 2003]

Control alternativo (Alternative control): Ver control mitigante

Control correctivo (Corrective control): Control definido para reducir o eliminar el impacto de incidente de seguridad ocurrido.

Control Detectivo (Detective control): Control definido para detectar la ocurrencia de un incidente de seguridad y permitir la reacción ante el mismo.

Control disuasorio (Dissuasive control): Control preventivo definido para hacer desistir a un potencial atacante antes de que se produzca el ataque.

Control general (Pervarsive control): Control que sirve de soporte para un conjunto amplio de activos, recursos y otros controles.

Control mitigante (Mitigating control): Control definido para suplir las deficiencias de otro control.

Control preventivo (Preventive control): Control definido para dificultar o impedir la ocurrencia de un incidente de seguridad.

Declaración de aplicabilidad (Statement of Applicability, SOA): Documento formal en el que, para un conjunto de salvaguardas, se indica si son o no de aplicación en el sistema de información bajo estudio. Cfr. [MAGE06] (Bajo la entrada "Documento de selección de controles")

Degradación (Degradation): Pérdida del valor de un activo como consecuencia de la realización de una amenaza. Cfr. [MAGE06]

Disponibilidad (Availability): Propiedad de la información y sus activos asociados sea accesible y utilizable bajo la demanda por una entidad autorizada. Cfr. [MAGE06], Cfr. [ISO27002.05], Cfr. [ISO7498-2.89]

Efectividad (Effectiveness): Ver eficacia.- Es la capacidad de lograr un efecto deseado o esperado.

Eficacia (Effectiveness): Propiedad de que se cumplen todos los objetivos de negocio definidos para un determinado elemento. Cfr. [ISACA07].

Eficiencia (Efficiency): Propiedad de que un requerimiento de negocio se alcanza realizando un consumo óptimo de los recursos disponibles para ello. Cfr. [ISACA07].

Entregar y Dar Soporte (DS).- 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 operacionales. Por lo general aclara las siguientes preguntas de la gerencia ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?, ¿Están optimizados los costos de TI?, ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?, ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad? [COBIT, 2005].

Escenario de riesgos (Risk scenario): Descripción del efecto de un conjunto determinado de amenazas sobre un determinado conjunto de activos, recursos y salvaguardas, teniendo en cuenta determinadas hipótesis definidas. Cfr. [ISO13335-1.04]

Estimación de riesgos (Risk estimation): Proceso utilizado para asignar valores de probabilidad e impacto asociados a un riesgo [ISO73.05]

Evaluación de riesgos (Risk evaluation): Comparación del riesgo estimado contra un determinado criterio para determinar su significatividad. [ISO73.05]

Evaluación de salvaguardas (Safeguard assessment): Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que mitigan. Cfr. [MAGE06]

Evidencia: Presentación de elementos (documentos, fotografías, correos electrónicos, etc.) que se agrega y usa para probar que el proceso y la actividad de control se están llevando a cabo adecuadamente.

Evitación (Avoidance): Estrategia de gestión de riesgos que consiste en eliminar los activos y los recursos que suponen un riesgo superior al considerado tolerable.

Fiabilidad (Reliability): Propiedad de mantener de forma consistente un comportamiento y unos resultados. Cfr. [ISO13335-1.04]

Frecuencia (Frecuency): Tasa de ocurrencia de una amenaza. [MAGE06]

Gestión de riesgos (Risk Management, Risk treatment): Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [MAGE06], Cfr. [ISO13335-1.04], Cfr. [ISO27002.05].

Impacto (Impact): Consecuencia potencial que sobre un activo tiene la realización de una amenaza. Cfr. [MAGE06]

Impacto residual (Residual Impact): Consecuencia potencial que sobre un activo tiene la realización de una amenaza, una vez considerados los efectos mitigantes de las salvaguardas implantadas.

Incidente (Incident): Evento inesperado o indeseado que puede causar un compromiso de las actividades de negocio de la seguridad de la información [ISO13335-1.04]

Integridad (Integrity): Propiedad de que la información y los métodos de procesamiento sean exactos y completos. Cfr. [MAGE06], Cfr. [ISO13335-1.04], Cfr.-[ISO27002.05]

Línea base de controles: (Controls baseline): Conjunto mínimo de salvaguardas definido para un sistema u organización. [ISO13335-1.04]

Mapa de riesgos (Risk map): Relación de las amenazas valoradas a las que están expuestos los activos. Cfr. [MAGE06]

Mapeo de procesos: Una aproximación que define la organización como un sistema de procesos interrelacionados. El mapa de procesos impulsa a la organización a poseer una visión más allá de sus límites geográficos y funcionales, mostrando como sus actividades están relacionadas con los clientes externos, proveedores y grupos de interés. Tales ¨mapas¨ dan la oportunidad de mejorar la coordinación entre los elementos clave de la organización. Así mismo dan la oportunidad de distinguir entre procesos clave, constituyendo el primer paso para seleccionar los procesos sobre los que actuar.

Marco de control.- Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Métrica: Un estándar para medir el desempeño contra la meta, [COBIT, 2005]

Monitorear y Evaluar (ME).- 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 de desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia: ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?, ¿La gerencia garantiza que los controles internos son efectivos y eficientes?, ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?, ¿Se miden y reportan los riesgos de control, el cumplimiento y el desempeño? [COBIT, 2005]

Normativa de seguridad (Security regulation): Conjunto de documentos que desarrollan la política de seguridad.

Objetivos.- Declaraciones generales establecidas por los auditores que definen los logros pretendidos del trabajo, [COBIT, 2005]

Objetivo de punto de recuperación (Recovery Point Objetive): Punto en el que un determinado proceso se recupera tras un incidente. Determina el volumen tolerable de transacciones que puede perderse en caso de un incidente.

Objetivo de tiempo de recuperación (Recovery Time Objetive): Período de tiempo objetivo definido para recuperar el funcionamiento de un determinado proceso tras un incidente. Cfr. [BS25999-1.06]

Pérdida anual esperada (Annual lose expectancy): Pérdidas anuales estimadas por la realización de una determinada amenaza sobre un recurso de información.

Pérdida esperada.- (Single lose expectancy): Pérdidas estimadas por la realización de una determinada amenaza sobre un recurso de información.

Plan de continuidad de negocio (Business continuity plan): Colección documentada de procedimientos e información desarrollada, recopilada y mantenida de modo que esté disponible para su uso en caso de incidentes y permita a la organización continuar la ejecución de sus actividades críticas a un nivel aceptable predefinido.[BS25999-1.06]

Plan de recuperación de desastres (Disaster Recovery plan): Conjunto de medidas definidas para recuperar un determinado servicio de soporte al negocio tras una interrupción provocada por un incidente.

Plan de seguridad (Security plan): Conjunto de proyectos de seguridad priorizados y presupuestados que permiten materializar las decisiones de gestión de riesgos. Cfr. [MAGE06]

Planear y Organizar (PO).- Este dominio cubre las estrategias y las tácticas, tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización d la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia. ¿Están alineadas las estrategias de TI y del negocio?, ¿Entienden todas las personas dentro de la organización los objetivos de TI?, ¿Se entienden y administran los riesgos de TI? ¿Es apropiada la calidad de los sistemas de TO para las necesidades del negocio? [COBIT, 2005]

Política de seguridad (Security policy): Conjunto de reglas, directivas y prácticas que gobiernan cómo se gestionan, protegen los activos y recursos de información. Cfr. [ISO13335-1.04]

Probabilidad (Likelihood): Medida de expectativa de que una amenaza se realice en un período de tiempo determinado, generalmente un año.

Proceso de gestión de la seguridad (Security Management process): Conjunto de objetivos, recursos, funciones, responsabilidades y tareas definidos para garantizar la seguridad de una organización.

Proyecto de seguridad (Security Project): Conjunto de actividades interrelacionadas definidas para logra un determinado objetivo en relación a la mejora o mantenimiento del nivel de seguridad de la información.

Recurso de información (Information Resource): Cualquier elemento empleado en el tratamiento de activos de información.

Nota: en general los estándares de análisis de riesgos no diferencian la información como concepto abstracto y los recursos físicos y lógicos utilizados para su tratamiento, considerando ambos bajo el concepto de activos de información. En el contexto de este proyecto, se considera activo de información el concepto abstracto de la información necesaria para el funcionamiento de la organización y se considera recurso de información los medios físicos y lógicos utilizados para el tratamiento.

Reducción (Reduction): Estrategia de gestión de riesgos que consiste en la aplicación de salvaguardas para reducir un riesgo cuyo nivel supera el umbral de riesgo tolerable definido.

Requerimiento de seguridad (security Requirement): conjunto de propiedades de la información y sus recursos cuyo incumplimiento supone un incidente que tiene como consecuencia un daño para un sistema o la organización.

Riesgo (Risk): Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización [MAGE06]

Riesgo acumulado (Accumulated Risk): Riesgo calculado tomando en consideración el valor propio de un recurso de información y el valor de los activos de información que dependen de él. Este valor se combina con la degradación y la frecuencia de las amenazas del recurso de información considerado. Cfr. [MAGE06]

Riesgo efectivo (Effective Risk): Riesgo remanente en el sistema tras la valoración de las salvaguardas actualmente implantadas.

Nota: si bien este término se considera habitualmente como sinónimo de riesgo residual, en el contexto de este proyecto se utiliza con significado distinto, diferenciado el riesgo calculado

teniendo en cuenta las salvaguardas implantadas del riesgo calculado teniendo en cuenta las salvaguardas previstas en el plan de seguridad.

Riesgo intrínseco (Intrinsic Risk): Riesgo en el sistema sin valorar la eficacia de las salvaguardas implantadas o incluidas en el plan de seguridad [MAGE06]

Riesgo repercutido (Affected Risk): Riesgo calculado tomando en consideración únicamente el valor propio de un activo de información. Este valor se combina con la degradación y la frecuencia de las amenazas de los recursos de información de los que depende. Cfr. [MAGE06].

Riesgo residual (Residual Risk): Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información [MAGE06]

Salvaguarda (Safeguard): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a un sistema o a la organización. Cfr. [MAGE06]

Seguridad de la información (Information Security): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los activos de información de una organización. Cfr. [MAGE06]

Sistema de gestión de seguridad de la información (Information Security Management Systems): Herramienta a disposición de la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad. Comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Está basado en el ciclo de la mejora continua (PDCA). Cfr. [UNE71502.04]

Tolerancia al riesgo (Risk tolerance): Cantidad de riesgo que una Organización es capaz de gestionar.

Transferencia (Transfer): Estrategia de gestión de riesgos que consiste en transferir un riesgo a una entidad externa que deba encargarse de su gestión y que asuma los daños en caso de ocurrencia de un incidente.

Valor (Value): Estimación de la utilidad de un determinado activo de información para la organización, teniendo en cuenta los diferentes requerimientos de seguridad definidos.

Valor acumulado (Accumulated Value): Valor de un determinado recurso de información teniendo en cuenta el valor de los activos de información que dependen de él. Cfr. [MAGE06]

Vulnerabilidad (Vulnerability): Debilidad en un recurso de información que puede ser explotada por una amenaza para causar un daño a un sistema o a la Organización. Cfr. [ISO27002.05]

GLOSARIO ABREVIATURAS, SIGLAS Y ACRÓNIMOS

En este glosario se presentan las abreviaturas de uso frecuente en este documento y en el dominio del análisis y la gestión de riesgos de seguridad de la información.

ARO: Determinación de la frecuencia anual

ALE: Determinación de la expectativa de pérdida anual

AGR: Análisis y Gestión de Riesgos

BCP: Business Continuity Plan, plan de continuidad de negocio

BS7799: Estándar creado por British Standards Institute (BSI), titulado ¨Information Security Management Systems¨ (Administración de Seguridad en sistemas de información).

CEO: Chief Executive Officer (Director General)

CFO: Chief Financial Officer (Director Financiero)

CIO: Chief Information Officer (Director de Información)

BIA: Business Impact Analysis, análisis de impacto sobre el negocio.

BMV: Bolsa Mexicana de Valores

BSI: British Standards Institute, Instituto Británico de Estándares

C.C.V: Central de Contraparte de Valores

CMM: Capability Maturity Model, modelo de madurez de capacidades.

C.N.V: Consejo Nacional de Valores

COBIT: The Control Objectives for Information and related Technology (Objetivos de Control para la información y tecnología relacionada).

COCO: Canadian Criteria of Control Committee

CONTROL TURNBULL: Internal Control Guidance for Directors on the Combined Code-UK (Guía de control interno para directores).

COSO: Internal Control – Integrated Framework del Committee of Sponsoring Organizations of the Tread way Commission (Estándar de Control Interno desarrollado por el Comité de Organizaciones patrocinadoras de la comisión Tread way.

DFD: Data Flow Diagram (Diagrama de Flujo de Datos)

DRP: Disaster Recovery Plan, plan de recuperación de desastres

ERP: Enterprise Resource Planning (Software integral-Planeación de Recursos empresariales)

INDEVAL: Instituto de Depósito de Valores

ISACA: Information Systems and Audit Control Association (Asociación de Auditoria y Control de Sistemas de Información.

ISMS: Information Security Management Systems, Sistema de gestión de seguridad de la información.

ISO: International Organization for Estandarización, Organización Internacional de Estandarización

ITGI: Information Technology Governance Institute. (Comité de Investigación del Instituto de Gobierno de TI).

ITIL: Information Technology Infrastructure Library (Conjunto de mejores prácticas para las tecnologías de la Información).

.

NIST. - National Institute of Standards and Technology

PCN: Plan de continuidad de negocio

PDCA: Plan, Do, Check, Act. Planificar, Ejecutar, Comprobar, Actuar. Ciclo de Deming o de mejora continua.

PRD: Plan de recuperación de desastres.

RACI: Responsible, Accountable, Consulted, and Informed. Encargado, responsable, consultado, informado.

RNV: Registro Nacional de Valores

ROSI: Rendimiento de la inversión en seguridad

SAC: Systems Auditability and Control del Institute of Internal Auditors research foundation (Sistemas de Auditoria y Control).

SAP: Systems Anwendungen and Produkte (Sistemas, Aplicaciones y Productos).

SGSI: Sistema de Gestión de Seguridad de la Información.

SLE: Determinación de la expectativa de pérdida simple

SOA: Statement of Applicability, declaración de aplicabilidad

SOX: Ley Sarbanes Oxley

T.I.: Tecnología de Información

WAN: World Área Network (Red de Área Mundial)