UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS

CARRERA DE CONTADURIA PÚBLICA

MODELO DE GESTIÓN DE RIESGOS DE TI

BAJO COBIT 5

Tesis de Grado presentado para la obtención del Grado de Licenciatura

POR: RUDDY CHAMBI CHOQUE

TUTOR: Mg. Sc. MIGUEL COTAÑA MIER

LA PAZ – BOLIVIA

2018

DEDICATORIA:

Dedico el presente trabajo:

A mi padre, que con su ejemplo y apoyo va marcando con huellas profundas mi camino.

A mi amada madre, por su infinito amor y comprensión.

A mi esposa por su fuerza y su inquebrantable optimismo y determinación.

Ruddy Chambi Choque

AGRADECIMIENTO

En primer lugar, agradezco a DIOS por darme salud, fuerza y llenar mi vida de bendiciones.

A mi tutor de Tesis de Grado Mg. Sc. Miguel Cotaña Mier por la orientación necesaria para realización de este trabajo.

A mi hermosa familia por todo su apoyo incondicional.

Ruddy Chambi Choque

ÍNDICE DE CONTENIDO

CAPÍTULO I

MARCO INTRODUCTORIO

CAPÍTULO II

MARCO INSTITUCIONAL

CAPÍTULO III
MARCO TEÓRICO

CAPÍTULO IV
DESARROLLO DEL MÉTODO

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El análisis de riesgos es parte de la planeación de la auditoria y ayuda a identificar los riesgos y las vulnerabilidades para que el Contador Público pueda determinar los controles necesarios para mitigarlos.

El Presente trabajo constituirá un modelo de Gestión de Riesgos de Tecnología de Información (TI) basado en COBIT 5 que coadyuve con el control de la planeación estratégica del negocio, facilitando la detección de áreas críticas dentro de la organización, estableciendo límites y mecanismos de control y mitigación de los niveles de exposición a los diferentes riesgos

La presente investigación es el aporte en el ámbito de las TI con la propuesta de un modelo de implantación de COBIT 5 para la gestión de riesgos de las TI. Esta propuesta nace a partir de la necesidad de contar con un instrumento que nos permita gestionar los riesgos de TI a nivel estratégico. Además, puede convertirse en una fuente de documentación sobre el tema y en una herramienta para la gestión de Riesgos de TI basada en COBIT 5.

Una vez que se culmine la Gestión de Riesgos bajo COBIT 5, en base a todos los procedimientos descritos en el marco de trabajo (Recopilar Datos, Analizar, Mantener Perfil, Expresar, Definir Acciones y Responder), el Contador Público podrá garantizar que los riesgos para el negocio relacionados con TI no exceden el nivel aceptable establecido por la dirección y que el impacto de los riesgos inherentes a TI que podrían afectar al negocio son gestionados y que la probabilidad de potenciales incumplimientos a leyes es minimizada**.**

Palabras Claves: Modelo, Gestión, Riesgo, COBIT 5, Tecnología, Información

SUMMARY

Risk analysis is part of the planning of the audit and helps to identify the risks and vulnerabilities so that the Public Accountant can determine the controls necessary to mitigate them.

The present work will constitute a model of Information Technology (IT) Risk Management based on COBIT 5 that helps control the strategic planning of the business, facilitating the detection of critical areas within the organization, establishing limits and control mechanisms and mitigation of exposure levels to different risks

The present research is the contribution in the field of IT with the proposal of a COBIT 5 implementation model for IT risk management. This proposal was born from the need to have an instrument that allows us to manage IT risks at a strategic level. In addition, it can become a source of documentation on the subject and a tool for managing IT Risks based on COBIT 5.

Once the Risk Management under COBIT 5 is completed, based on all the procedures described in the framework (Collect Data, Analyze, Maintain Profile, Express, Define Actions and Respond), the Public Accountant can guarantee that the risks for the business related to IT they do not exceed the acceptable level established by the management and that the impact of the inherent risks to IT that could affect the business are managed and that the probability of potential breaches of laws is minimized.

Keywords: Model, Management, Risk, COBIT 5, Technology, Information

CAPITULO I

MARCO INTRODUCTORIO

CAPÍTULO I

MARCO INTRODUCTORIO

1.1. INTRODUCCIÓN

El entorno actual está marcado por la aceleración vertiginosa de la tecnología, la rapidez en los cambios sociales, económicos y políticos, y la necesidad de creación de valor.
La tecnología, es la aplicación de los nuevos conocimientos de la ciencia al mejoramiento de la industria. Es la habilidad del ser humano de aprovechar ciertas herramientas para un mejor estilo de vida.

La Tecnología de la Información (TI) es una de las diversas herramientas que utiliza la alta gerencia para lidiar con el cambio: Hardware, Software, almacenamiento de datos, redes y telecomunicaciones, Tecnologías de la Información y Comunicación (TIC), Nuevas Tecnologías de la Información y Comunicación (NTIC). Todas estas tecnologías, junto con las personas requeridas para operarlas y administrarlas, representan recursos que se pueden compartir en toda la organización y constituyen la infraestructura de tecnología de la información (TI) de la empresa. La infraestructura de TI provee la base, o plataforma, sobre la que una empresa puede crear sus Sistemas de Información (SI) específicos.

Las TIC ejercen una influencia directa en la productividad y competitividad organizacional. Son consideradas recursos estratégicos vitales, para el desarrollo de cualquier organización. Sin embargo, como cualquier recurso, es vulnerable a múltiples amenazas que se pueden materializar en riesgos[1], con diversos impactos en términos de pérdida de información, interrupción de servicios, pérdidas financieras, daños a la reputación e incluso pérdidas humanas.

[1] Efecto de la incertidumbre en la consecución de los objetivos. (ISO 31000:2009)

El análisis de riesgos es parte de la planeación de la auditoria y ayuda a identificar los riesgos y las vulnerabilidades para que el Contador Público pueda determinar los controles necesarios para mitigarlos.

Amenazas tan comunes como los virus, spyware, spam, adware, malware, ransonware, troyanos, gusanos hasta amenazas tan sofisticadas como las denominadas amenazas persistentes avanzadas (APT, por sus siglas en inglés Advanced Persistent Threat), o los ataques día cero (en inglés, zero-day attack) a las cuales está expuesta cualquier organización, lleva a la necesidad de valorarlos y a partir de allí tomar acciones que permitan implementar adecuados controles para tratar de garantizar niveles aceptables de riesgo.

En el mundo educativo y de negocios, debido a que nos enfrentamos a entornos cambiantes donde las decisiones que tomamos siempre tienen un grado de incertidumbre, el riesgo acaba siendo un elemento inherente a nuestra actividad. No podemos eliminarlo, pero sí podemos aprender a gestionarlo y a reducirlo.

El riesgo es parte de todas nuestras vidas. Como sociedad, debemos tomar riesgos para crecer y desarrollarnos.

Existen diferentes tipos de riesgo: financiero, crediticio, operacional, tecnológico, estratégico, de mercado, de seguridad de la información, de seguridad de los aeropuertos, de continuidad del negocio, de auditoría entre los más relevantes.

En nuestro mundo acelerado, los riesgos que tenemos que gestionar evolucionan rápidamente. Necesitamos asegurarnos de gestionar los riesgos de manera que podamos minimizar sus amenazas y maximizar su potencial. ¡La gestión de riesgos de TI, es algo del día a día!

En términos del Riesgo Tecnológico, existe consenso generalizado en definirlo como: la posibilidad de pérdidas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la organización, al comprometer o degradar las dimensiones críticas de la información, tales como la:

- Confidencialidad;
- Integridad;
- Disponibilidad.

En ese sentido, COBIT[2] 5 para Riesgos define el Riesgo de TI como un riesgo para el negocio, específicamente el riesgo para el negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de TI dentro de una empresa.

COBIT 5, se focaliza en la "maximización de la creación de valor a partir de TI para el negocio" mediante el cumplimiento simultáneo de tres objetivos de gobierno: maximización de beneficios, optimización de recursos y optimización de riesgos.

La introducción del concepto de optimización de riesgos como objetivo de gobierno, muestra una clara evolución frente al enfoque tradicional de mitigación de riesgos, más basada en la visión clásica de la auditoría.

Concretamente, COBIT 5 define la optimización de riesgos como "garantizar que los riesgos para el negocio relacionados con TI no exceden el nivel aceptable establecido por la dirección y que el impacto de los riesgos inherentes a TI que podrían afectar al negocio son gestionados y que la probabilidad de potenciales incumplimientos a leyes es minimizada**".**

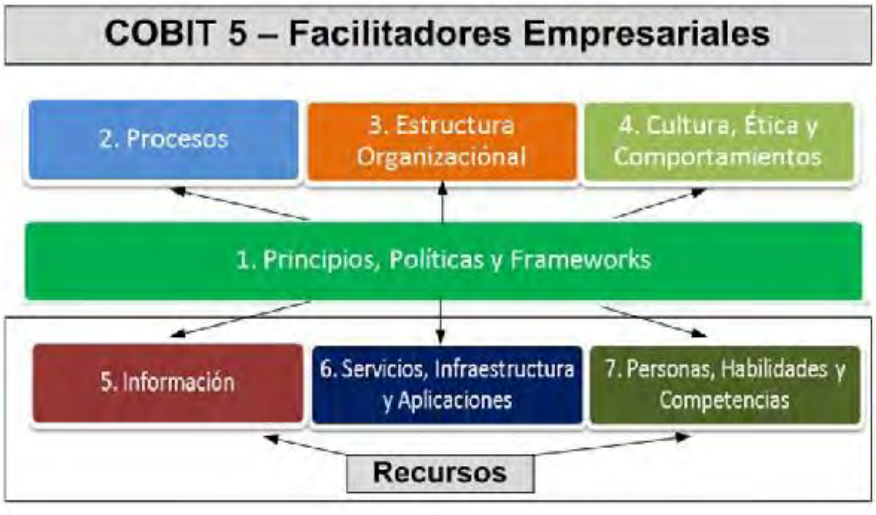
[2] COBIT (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de TI y mejorar los controles de TI. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

Es razonable pensar que las organizaciones deben integrar la gestión del riesgo tecnológico en una forma mucho más efectiva y concreta dentro de la gestión del riesgo empresarial (ERM), si quieren reducir sus futuras pérdidas y mejorar la performance del negocio.

No es suficiente identificar un riesgo y agregarlo al registro de riesgos, es fundamental poder vincularlo directamente con el resultado de los objetivos estratégicos para el Negocio.
Una inadecuada gestión de los riesgos de TI puede reducir el valor del negocio, creando pérdidas financieras, dañando la reputación corporativa y desperdiciando nuevas oportunidades.

En base los aspectos fundamentales de ISO 27000, ISO 31000, COBIT 5, y COSO. Este proyecto tiene la finalidad de promover un gobierno de TI y, por ende, de esta manera, lograr una mejor gestión del riesgo al que pueden estar expuestas hoy en día las empresas. Con ese objetivo, el presente trabajo propone un modelo de Gestión de Riesgos de TI bajo COBIT 5, que brindará una guía detallada para gobernar y gerenciar los Riesgos de TI en base a lineamientos (ver figura 1.1) para la gestión y gobierno del riesgo informático.

Figura 1. 1: Facilitadores Empresariales



Fuente: COBIT 5. Facilitadores empresariales

1.2. ANTECEDENTES Y TRABAJOS PREVIOS

Satisfacer criterios de confidencialidad, disponibilidad e integridad de la información financiera constituyen el objetivo fundamental de la Ley Sarbanes-Oxley. Mucho de lo que se ha escrito sobre la estructuración de un adecuado modelo de control interno está orientado a satisfacer de forma razonable los objetivos corporativos; sin embargo, los modelos propuestos se centran en las actividades operativas y transaccionales, olvidándose de la importancia de la información. La tendencia de las organizaciones modernas es a automatizar todo proceso o actividad haciendo uso de herramientas basadas en TI, esto genera una dependencia creciente que se incrementa al vincular otros actores externos a los sistemas informáticos corporativos. Obviamente esta estrategia, que apunta a ganar eficiencia y eficacia en los procesos, genera grandes vulnerabilidades a las que las empresas deberán responder de forma efectiva.

COBIT 5 es la nueva versión del marco de trabajo más reconocido a nivel internacional orientado al negocio para el gobierno y el management de TI con visión empresarial:

- Incorpora las mejores prácticas en términos de Governance, Risk & Compliance de IT, las cuales son habitualmente consideradas para futuras regulaciones al respecto de los distintos organismos de control;
- Incluye las perspectivas de TI desde el directorio, desde auditoría y desde las gerencias del negocio;
- Es altamente customizable, flexible y provee las estructuras y herramientas que los líderes de las empresas necesitan para brindar valor al negocio;
- COBIT 5 ayuda a los ejecutivos a obtener más ventajas desde los sistemas de información vigentes y provee un enfoque simplificado, con una visión integral, para el gobierno y la gestión de TI provee las herramientas y modelos para ayudar a los líderes de las empresas a gestionar riesgos en forma efectiva, asegurar cumplimiento, brindar continuidad, seguridad y privacidad en los aspectos relacionados con la información y la tecnología.

Existen riesgos en todo lo que hacemos y de igual manera, las organizaciones tienen que enfrentarlos para alcanzar sus objetivos.

TI se ha convertido en un elemento estratégico para crear oportunidades, innovación y ventaja competitiva, pero a su vez conlleva riesgos inherentes que requieren atención en la entrega de servicios, proyectos y en las iniciativas de negocios habilitados por TI; por lo que los riesgos deben ser gobernados y gestionados.

A la alta gerencia le corresponde establecer el gobierno y la cultura organizacional hacia los riesgos, definir los criterios y el apetito o nivel de riesgo que la organización está dispuesta a aceptar para lograr sus objetivos; así como su tolerancia, y asegurar que los riesgos se gestionen. La mejor manera de hacerlo es estableciendo directrices claras mediante políticas y liderando con el ejemplo.

La gestión de riesgos implica su identificación, análisis y evaluación para darles un tratamiento apropiado y así, llevarlos a un nivel aceptable para la organización. La respuesta puede ser mitigar o reducir el riesgo, transferirlo o compartirlo, evitarlo o aceptarlo.
De la investigación efectuada, se ha podido consultar los siguientes trabajos existentes en la biblioteca de la Carrera de Contaduría Pública:

TÍTULO	Auditoria de confiabilidad sobre los riesgos y estados financieros del viceministerio de desarrollo Rural y Agropecuario - Administración de activos fijos - Gestión 2008
AUTOR	Quelali Condori, Nelly María
GESTIÓN	2011
DESCRIPCIÓN	El presente trabajo titulado "Auditoria de confiabilidad sobre los Registros y Estados Financieros del Viceministerio de Desarrollo Rural y Agropecuario -

	Administración de Activos Fijos - Gestión 2008, se realizó la auditoria al Viceministerio de Desarrollo Rural y Agropecuaria con la finalidad de verificar la adecuada administración de los recursos y aplicación de la normativa que regula al sector público. En tales circunstancias la motivación que llevo a realizar este trabajo es la de poder identificar y aportar con algunos criterios correctivos que permitan un adecuado control y administración de los activos fijos en el Viceministerio de Desarrollo Rural y Agropecuario. Durante el examen se pudo evidenciar que el viceministerio de Desarrollo Rural y Agropecuario no cuenta con una adecuada administración de activos fijos ya que se detectó que existe ausencia de control en la asignación y devolución de los activos fijos, se encontraron activos sin custodios, no todo el personal contaba con su acta de asignación, existían activos que no eran de propiedad de Viceministerio, por lo que se llegó a la conclusión de que el personal de la institución ya sea eventual o permanente desconocía la normativa de uso de activos fijos, existía rotación de personal que ocasionó el descontrol de los activos y finalmente se evidenció la necesidad de contar con espacios de almacenaje y suficiente personal que mantenga un inventario actualizado el cual brinde una información exacta y oportuna. Para que se pueda lograr una gestión eficiente en la administración de los activos fijos se recomendó lo siguiente: a Nivel de registro contable,

	realizar un levantamiento de todos los activos fijos y documentar tanto las salidas como los ingresos de los mismos, a nivel del personal y manejo de la normativa, debe contar con suficiente personal el mismo a la vez debe estar capacitado y tener conocimiento del manejo de activos y lo más primordial dar a conocer a todo el personal la normativa que rige a la administración de los activos fijos.

Fuente: Biblioteca de la Carrera de Contaduría Pública

TÍTULO	La auditoría de gestión de calidad y gestión de riesgos en las organizaciones. Caso: Ministerio de Trabajo
AUTOR	Aliaga Echave, Marco Antonio
GESTIÓN	2007
DESCRIPCIÓN	En el contexto económico actual donde se destaca la competitividad y globalización de los mercados, los modelos de calidad han evolucionado hacia una consecución de la excelencia de la gestión. Así, cada vez un mayor número de organizaciones adoptan planteamientos para mejorar su gestión y asumen que la calidad supone una nueva forma de gestión empresarial para alcanzar la eficiencia económica. En virtud de lo anterior, la auditoría de gestión de calidad pasa a ser hoy por hoy un elemento vital para la gerencia, permitiéndole conocer a los ejecutivos el grado de la organización alcanza los estándares o medidas de calidad establecidas en sus políticas o sistemas de calidad, generando en la empresa un saludable dinamismo que la conduce

	exitosamente hacia las metas propuestas. Desde el punto de vista teórico, el trabajo de investigación tiene su sustento en la gestión de calidad, que es conceptuado como "las actividades coordinadas para dirigir y controlar una organización en lo relativo a la calidad", en este caso dentro del ámbito de la administración pública, donde la calidad debe entenderse como un proceso de gestión de cambio, como una transformación que supone la revisión de la estructura organizativa, la concepción de los recursos humanos, los procesos. Para tal cometido, es imprescindible la utilización del método científico y técnicas apropiadas en la recolección de información, para facilitar la relación del trabajo con el propósito de lograr resultados conforme a los objetivos de la investigación, y con la mayor confiabilidad posible, de tal manera que pueda confirmarse o desvirtuarse la hipótesis que orientara la presente investigación, para el efecto, se utilizará el método hipotético - deductivo, en razón de que la investigación será guiada por una hipótesis, que además permitirá delimitar el problema y finalmente deducir conclusiones. En este sentido, es una necesidad que las autoridades del nivel ejecutivo del ministerio de trabajo deban implementar sistemas, normas, sistemas y auditorias de calidad, como instrumento para mejorar su gestión y orientar la actividad estatal a la satisfacción de las necesidades y expectativas de la sociedad.

Fuente: Biblioteca de la Carrera de Contaduría Pública

TÍTULO	La importancia del control de gestión y riesgos para prevenir fraudes en las entidades de microcrédito
AUTOR	Alborta Gonzales, Ricardo
GESTIÓN	2014
DESCRIPCIÓN	El Riesgo de la industria del Microcrédito como factor interno y Externo siempre están presentes en el entorno, además que sus actividades se enmarca dentro de las prescripciones legales el ente regulador ASFI, sus operaciones están expuestas a diversos tipos de Fraude, actualmente los sistemas de Control deben dar una respuesta especifica ante este hecho delictivo e identificar los Riesgo que causan pérdidas cuantiosas a la institución. Cada Modelo de Control interno debe dar una respuesta clara de efectividad y eficiencia a la EIF, para ello se identifica el fenómeno fraude según los diferentes grupos que son: el fraude comercial, del empleado y el de Sistemas esto llega a los diferentes tipos de Riesgos Identificados que en las EIF, los más comunes son Riesgo de Mercado, Legal, Operativo, de Competencia, Tecnológico, Estratégico y de Responsabilidad Social, es importante aclarar que el riesgo es Inherente por la naturaleza de Giro de negocio que tiene cada EIF. Sin embargo es importante preguntarnos, ¿es posible coadyuvar el mejoramiento de los mecanismos de Control y gestión de riesgos? Si bien el Microcrédito tiene como objetivo el financiamiento a estas pequeñas unidades económicas pues debe cumplir si la función social y el desarrollo integral del "Vivir Bien" eliminar la

	pobreza y la exclusión social ligados y definidos con la Visión y Misión de la EIF sin embargo la ley de Servicios financieros regula la actividad a través de sus diversos reglamentos emitidos por ASFI, se desarrolla el Modelo denominado "Modelo de Control de Gestión de Riesgos Continuo", que no solo mitigara los porcentajes de Riesgo ante un fraude a la EIF sino también dará respuesta a una Buena Gestión de Riesgo Crediticio. Identificar los regímenes de previsiones de ASFI para este sector la constitución de previsiones de acuerdo la normativa vigente. Y los márgenes de Capital Regulatorio según los acuerdo de Basilea para un gobernabilidad convincente en las EIF s.

Fuente: Biblioteca de la Carrera de Contaduría Pública

TÍTULO	Método de gestión de riesgos para la auditoría de base de datos relacional
AUTOR	Sauter Estevez, Nitza
GESTIÓN	2016
DESCRIPCIÓN	Desde los comienzos de la computación, los recursos informáticos (incluyendo la información), han estado expuestos a una serie de peligros o riesgos que han aumentado y evolucionado conforme se globalizan las comunicaciones; de otro lado, el acceso a las Tecnologías de Información y Comunicaciones (TICs), ha generado un incremento en las oportunidades para obtener información, el cual a su vez es directamente proporcional al número de eventuales y posibles

	amenazas que de ello se desprenden. Estas amenazas exponen a las organizaciones a riesgos que pueden impactar la seguridad de los sistemas, la continuidad de las operaciones, la materialización de los fraudes (Internos o externos), producir daños en la infraestructura y la consecuente pérdida o alteración de información sensible, así como multas, sanciones, daños a la infraestructura, entre otros aspectos. Las Bases de Datos (BD) no protegidas son el sueño de cualquier ciberdelincuente. Contienen los datos más valiosos de la empresa, blanco fácil de un ataque. No es de extrañar que las bases de datos sean el objetivo principal de los ciberataques más sofisticado de los hackers y, cada vez más, de usuarios que trabajan en la empresa y que cuentan con determinados privilegios. Las bases de datos son el centro de atención para cualquier institución y/o empresa de hoy en día, ya que constituyen uno de los soportes fundamentales para el proceso de toma de decisiones gerenciales; de ahí la importancia de que los datos guardados en ellas sean confiables y de calidad. Uno de los procesos en la construcción de estas y que contribuye a lograr este objetivo, es la limpieza de los datos.

Fuente: Biblioteca de la Carrera de Contaduría Pública

1.3. PLANTEAMIENTO DEL PROBLEMA

La problemática del riesgo se encuentra asociada principalmente a los desarrollos científico-técnicos y a sus productos que dan cuerpo y funcionamiento a los diferentes procesos de modernización social y tecnológica.

La tecnología o las innovaciones tecnológicas entendidas como "objetos" forman parte de la sociedad. En ese entendido, desde el concepto de riesgo es posible cuestionar tanto la toma de decisiones ante la implementación de una tecnología o innovación, como también, las transformaciones que éstas pueden provocar en la vida cotidiana de las personas.
Los riesgos originados por eventos tecnológicos (la energía nuclear, los desechos radioactivos, los accidentes químicos, la contaminación tóxica, el cambio climático, la seguridad alimentaria, la seguridad de la información y los cultivos transgénicos, entre otros) son un componente propio de las sociedades modernas y que aún no encuentran las respuestas apropiadas en el quehacer científico, porque no es preciso determinar su eventualidad para prevenir futuros desastres ni su potencialidad.

Los avances tecnológicos han jugado un papel muy importante en las organizaciones, ya que han ayudado a las empresas a ser más eficientes en cuanto al ahorro y reducción de horas de trabajo y entrega de información de manera instantánea y eficiente. Aunque los procesos automatizados pueden ser eficientes y la información que se genera sea instantánea, siempre estarán presentes los riesgos en cada uno de los procesos con los que cuenta una organización, debido a que la tecnología surge de pensamientos y trabajo del hombre.

Un riesgo importante para tener en cuenta es el riesgo tecnológico, ya que a medida que pasa el tiempo, las empresas han estado llevando sus procesos a un nivel tecnológico superior, logrando automatizar sus procesos y llevándolas a ser más competitivas en los mercados actuales.

Usualmente, cuando se hace referencia a la palabra "riesgo", el significado que se le atribuye conlleva un carácter negativo relacionado con peligro, daño, siniestro o pérdida.
Sin embargo, el riesgo es parte inevitable de los procesos de toma de decisiones en general y de las decisiones de inversión en particular; los beneficios derivados de tomar una decisión o de realizar una acción cualquiera sea ésta, necesariamente deben asociarse con los riesgos inherentes a esa decisión o acción.

En forma específica, las TIC han dejado de ser tan solo herramientas de apoyo para convertirse en parte del negocio, y como tal ejercen una influencia directa en la productividad y competitividad organizacional. De allí que sean consideradas recursos estratégicos vitales, para el desarrollo de cualquier organización.

Dicho de otro modo, como cualquier recurso, es vulnerable a múltiples amenazas que se pueden materializar en riesgos, con diversos impactos en términos de pérdida de datos, interrupción de servicios, pérdidas financieras, daños a la reputación e incluso pérdidas humanas. Amenazas tan comunes como los virus, los fallos de software, las caídas de red, los programas espía, troyanos, los robos de equipos, el spam, hasta amenazas tan sofisticadas como las denominadas amenazas persistentes avanzadas, o los ataques día cero a las cuales está expuesta cualquier organización, lleva a la necesidad de valorarlos y a partir de allí tomar acciones que permitan implementar adecuados controles para tratar de garantizar niveles aceptables de riesgo. Todas las actividades orientadas a mantener niveles aceptables de riesgo en una organización, está en el marco de lo que se denomina gobierno y gestión del riesgo, en este caso en particular, y como parte del universo de riesgos organizacionales, todos aquellos procesos relacionados con los riesgos de TIC o TI, están en el marco del gobierno y gestión de riesgos de TIC.

La Gestión de Riesgos de TI es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles

adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo; minimizando su impacto en el negocio.

Lamentablemente, en nuestro país, la gestión de riesgos de TI es todavía muy incipiente o esfuerzos aislados que no van de la mano con los objetivos estratégicos institucionales, que buscan un proceso de mejora continua y de constante adaptación a los cambios en la organización en cuanto a procesos de negocio y a la tecnología implicada.

1.4. FORMULACIÓN DEL PROBLEMA

¿El desarrollo de un modelo de Gestión de Riesgos de Tecnología de Información basada en COBIT 5 proporcionará una herramienta lógica y formal para facilitar la detección de áreas críticas dentro de la organización, estableciendo mecanismos de control y mitigación de los niveles de exposición al riesgo?

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

Proponer un modelo de Gestión de Riesgos de Tecnología de Información (TI) basado en COBIT 5 que coadyuve con el control de la planeación estratégica del negocio, facilitando la detección de áreas críticas dentro de la organización, estableciendo límites y mecanismos de control y mitigación de los niveles de exposición a los diferentes riesgos.

1.5.2. OBJETIVOS ESPECÍFICOS

- Promover en las organizaciones un mayor grado de conciencia sobre la importancia de gestionar adecuadamente los riesgos a los que se enfrentan;
- Investigar fuentes bibliográficas referentes a la práctica de gestión de riesgos;

- Identificar y describir los riesgos de TI junto con las amenazas y vulnerabilidades que llevarían a la materialización de tales riesgos;
- Promover a un análisis adecuado del riesgo;
- El modelo puede ser utilizada por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, no es específica de una industria o sector concreto;
- Clasificar el nivel de impacto de los riesgos;
- Poder evaluar las áreas funcionales de la organización de acuerdo a macro riesgos, lo que dará como resultado una mejor administración de las áreas vulnerables;
- Ofrecer un método sistemático para analizar tales riesgos;
- Contar con métricas e indicadores de riesgos típicos en TI;
- Desarrollar el modelo.

1.6. DISEÑO METODOLÓGICO

Para desarrollar el presente trabajo, se utilizará investigación cualitativa, aplicando el: Método inductivo observacional y el deductivo basado en teorías.

1.6.1. TIPO DE INVESTIGACIÓN

Para el desarrollo del "Modelo de Gestión de Riesgos de Tecnología de Información bajo COBIT 5", basaremos nuestro estudio en el tipo de investigación explicativa.

1.6.2. PLANTEAMIENTO DEL DISEÑO DE INVESTIGACIÓN

El presente trabajo de investigación se basa en fuentes mixtas, por considerar en primera instancia la investigación documental (referencias de documentación impresa y de información disponible en Internet, documentos y/o bibliografía existente que sirva de base al estudio y al fundamento teórico).

La investigación documental se sustenta en la aplicación de diferentes técnicas como: Observación directa y participante, entrevistas, simulación, cuestionarios, análisis de la información disponible, revisión y análisis de normativa generalmente aceptada.

Las etapas por considerar:

ETAPA 1: Diseño del proceso de investigación (determinación de los objetivos y planteamiento del problema);
ETAPA 2. Recolección y descripción de la información (Trabajo de Campo aplicando técnicas de la observación, entrevistas y encuestas);
ETAPA 3. Clasificación y Análisis de Contenidos;
ETAPA 4. Interpretación;
ETAPA 5. Elaboración del informe final.

1.7. IMPORTANCIA Y JUSTIFICACIÓN DEL ESTUDIO

Toda organización tiene objetivos estratégicos, por lo general relacionados con el mercado y los negocios, y requiere que, desde los procesos de operaciones hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable.

Actualmente, pensar en una organización que no haga uso de las TI es prácticamente imposible. Pero ¿realmente este uso de TI está aportando valor agregado, o está contribuyendo realmente al logro de los objetivos en las organizaciones? ¿Pueden gestionar adecuadamente los activos institucionales?

El aseguramiento de los recursos con que cuenta una organización es uno de los objetivos de la gestión de riesgos, entendido éste como la posibilidad de que cualquier amenaza explote una vulnerabilidad específica para causar daño a un activo.

Muchos modelos de gestión, fundamentalmente en otros países, nos dicen QUE hacer, y hasta COMO hacer, pero pocos nos explican cómo gestionar adecuadamente los riesgos generados por las TI.
COBIT 5, puede ser una herramienta útil para este propósito. Aquí radica la importancia del proyecto de investigación. La principal justificación de la presente investigación es el aporte en el ámbito de las TI con la propuesta de un modelo de implantación de COBIT 5 para la gestión de riesgos de las TI. Esta propuesta nace a partir de la necesidad de contar con un instrumento que nos permita gestionar los riesgos de TI a nivel estratégico.

Este trabajo de grado se justifica porque puede convertirse en una fuente de documentación sobre el tema y en una herramienta para la gestión de Riesgos de TI basada en COBIT 5.

1.7.1. JUSTIFICACIÓN ECONÓMICA

El uso de un modelo y/o metodología para gestionar riesgos, agrega valor a la empresa, porque minimiza costos teniendo a disposición una referencia metodológica.

1.7.2. JUSTIFICACIÓN SOCIAL

Una nueva cultura de gobernabilidad da paso de una sociedad industrial a una sociedad de sobreabundancia de información y comunicación; pasar de la simple idea de mitigar riesgos y amenazas a la capacidad de gestionar los recursos de TI

1.7.3. VIABILIDAD

El alcance del objetivo de este trabajo de tesis será viable solo si los recursos humanos de la empresa u organización cambien de actitud. Y acepten que no podemos quedar aislados del resto del mundo en cuanto a la gestión de riesgos de TI.

1.8. ALCANCE Y APORTES

1.8.1. ALCANCE

Permitir que la Gestión de Riesgos sirva como punto de partida y auxilio para la planeación estratégica.

Dentro del alcance del proyecto, se presentará lo siguiente:

- El marco teórico de Gobierno y Gestión de TI enfocado en dos de los 5 dominios de COBIT 5:
  - Evaluar, Dirigir y Monitorear;
  - Alinear, Planear y Organizar;
  - Monitorear, Evaluar y Valorar;
  - Construir, Adquirir e Implementar;
  - Entregar, Servir y Dar Soporte;
- Procesos Habilitadores COBIT 5;
- Modelo de Evaluación de Procesos COBIT 5;
- Guía de Autoevaluación COBIT 5.

1.8.2. APORTES

Proponer y diseñar un modelo de gestión de riesgos de TI bajo COBIT 5.

CAPITULO II

MARCO INSTITUCIONAL

CAPÍTULO II

MARCO INSTITUCIONAL

2.1. ANTECEDENTE INSTITUCIONAL

El Instituto Tecnológico Marcelo Quiroga Santa Cruz inicio de forma experimental en 1986, como ISEC SUCRE (Instituto Superior de Educación Comercial "Mcal. Antonio José de Sucre", de acuerdo con el convenio interministerial entre el Ministerio del Interior, Migración y Justicia y el Ministerio de Educación y Cultura, con el propósito de elevar los niveles culturales, sociales y económicos de sectores desvalidos en situación de riesgo, a través de la educación.

Inicialmente se efectuaron estudios exploratorios, para detectar intereses, satisfacer necesidades y planificar los procesos de enseñanza-aprendizaje en las penitenciarias. Los principales impulsores para efectivizar dicho proceso educativo fueron los mismos primeros docentes, quienes gestionaron las primeras aulas en las celdas de los internos que así lo permitieron. Posteriormente y debido a la aceptación de la población penitenciaria, se coordinó con las autoridades internas del penal como también del Ministerio del Interior, para establecer un área educativa con aulas exclusivamente de enseñanza. Posteriormente en la segunda dirección del ISEC SUCRE a cargo de la directora Sra. Nelly Calla V. y el Lic. Carlos Sotomayor se gestionaron más ítems de docencia y dirección implementándose también más programas oficiales de enseñanza en las carreras comerciales a nivel técnico medio (Contador, Auxiliar de Contabilidad, Secretariado Administrativo y Auxiliar de Oficina).

Con el propósito de capacitar y lograr una efectiva rehabilitación de las personas privadas de libertad del penal de San Pedro el funcionamiento del ISEC SUCRE, se legaliza por Resolución Ministerial Nº 1293 del 25 de septiembre de 1991, como Anexo del ISEC "LA PAZ", Bajo convenios interinstitucionales entre: El Ministerio de Educación y la Dirección

de Régimen Penitenciario. Dando también cumplimiento a Disposiciones Internacionales como la Resolución 1990/20 del 24 de mayo de 1990 emitida por el Consejo Económico y Social de las Naciones Unidas y la Subdivisión de Prevención del Delito y Justicia Penal de la Secretaria de las Naciones Unidas, además del Consejo Internacional de Bienestar Social y el Consejo Internacional de Educación de Adultos de la UNESCO – 1995, sobre la inclusión de Programas de Alfabetización, Educación Básica, Formación Profesional, Educación Social, Enseñanza Superior, y Actividades Religiosas Culturales y Deportivas en establecimientos penitenciarios, orientadas a la rehabilitación e reintegración social de las personas privadas de libertad, con la finalidad de proporcionar una educación susceptible de producir y promover actitudes positivas, promover la estabilidad y el sentido de dignidad.

Todo el proceso de formación profesional integral que ofrece, y al que se acogen los estudiantes se respalda en la LEY DE EJECUCIÓN PENAL 2298 y su beneficio de "redención" estipulado en sus artículos 138,139,140 y 141 Cap. III (Ley del 2 x 1 Redención de Penas) en el que se estipula la redención de un día de pena por dos días de estudio o trabajo, debidamente certificados a los internos que cumplan los con los requisitos.

Hasta la gestión 2009 el instituto tuvo como directores: Sra. Magda, Lic. Nelly Calla, Dr. Edgar Canaviri, Lic. Omar Barrera A. y la Lic. Aurea Balderrama A., a quien y por intervención de las autoridades del SEDUCA, se le instruye iniciar un proceso de reordenamiento técnico pedagógico y administrativo, momento en el cual el ISEC SUCRE, tiene como oportunidad proyectarse también fuera de los centros penitenciarios; y así brindar mayor cobertura educativa no solo para los estudiantes internos que obtengan su libertad y puedan integrarse en el ISEC SUCRE afuera, para la continuidad y culminación de sus estudios; sino también se expande a nuevos sectores de las laderas de la zona Villa Nuevo Potosí, Av. 9 de abril, curva Mururata, donde las organizaciones sociales de la zona gestionaron la construcción de una infraestructura acorde a los requerimientos de una institución de formación Técnico Tecnológica, misma que el ISEC SUCRE tuvo el privilegio de estrenar como suya para implementar carreras industriales.

Es así que el ISEC SUCRE, bajo la dirección de la Lic. Aurea Balderrama A., se elabora y presenta el proyecto educativo institucional, iniciándose las gestiones para el:

- Cambio de Razón Social, a "INSTITUTO TECNOLOGICO MARCELO QUIROGA SANTA CRUZ",
- Apertura de su Sede Central en la zona de Villa Nuevo Potosí, curva Mururata, Av. 9 de abril N° 1060. Y su Sub Sede en los Centros Penitenciarios de Departamento de La Paz.
- Regulación y validación de carreras a nivel Técnico Superior,
- Implementación de carreras industriales como: Electricidad Industrial, Sistemas Informáticos y Construcción Civil, en la Sede Central.
- Validación de las carreras comerciales como: Contaduría General y Sistemas Informáticos, en la Sub Sede de San Pedro.

Finalmente, y después de un largo proceso burocrático durante 3 años de lucha por mantener los derechos a la educación de las personas privadas de libertad, nuestra nueva resolución ministerial Nº 039/13, es emitida en febrero del año 2013.

A partir de la nueva resolución se inician las gestiones para el Equipamiento de los Talleres en las Carreras Industriales Sede Central, el equipamiento de Laboratorios de Computación en la Sub Sede de San Pedro. Implementación de Salas Audiovisuales con Data Show en ambas Sedes y la participación oficial en eventos Culturales y Deportivos en representación a nivel local y departamental, sentando precedente de ser la única institución a nivel Nacional, con presencia educativa de formación profesional técnica superior en los Centros Penitenciarios del Departamento de La Paz, como sub sedes.

2.2. CONFORMACIÓN JURÍDICA Y ADMINISTRATIVA

2.2.1. IDENTIFICACIÓN DE LA EMPRESA

La empresa se identifica con los siguientes datos:

Razón social	:	Instituto Tecnológico Marcelo Quiroga Santa Cruz
Rama-actividad	:	Educación
Subsector	:	Educación Superior
Tipo de empresa	:	Institución Fiscal
Resolución Ministerial	:	R.M. 039/13
Composición del capital	:	Asignación Presupuestaria Gobierno Autónomo Departamental de La Paz – Recursos Propios

2.2.2. UBICACIÓN GEOGRÁFICA

El Instituto Tecnológico Marcelo Quiroga Santa Cruz está ubicado en la avenida 9 de abril, Curva Mururata N.º 1060 Zona Villa Nueva Potosí, (ver figura 2.1 y 2.2) ofertando carreras anuales y semestrales con laboratorios y talleres. Asimismo, cuentan con un cuerpo de docentes especializados.

Figura 2. 1: Dirección Instituto Tecnológico Marcelo Quiroga Santa Cruz

Fuente: Elaboración propia

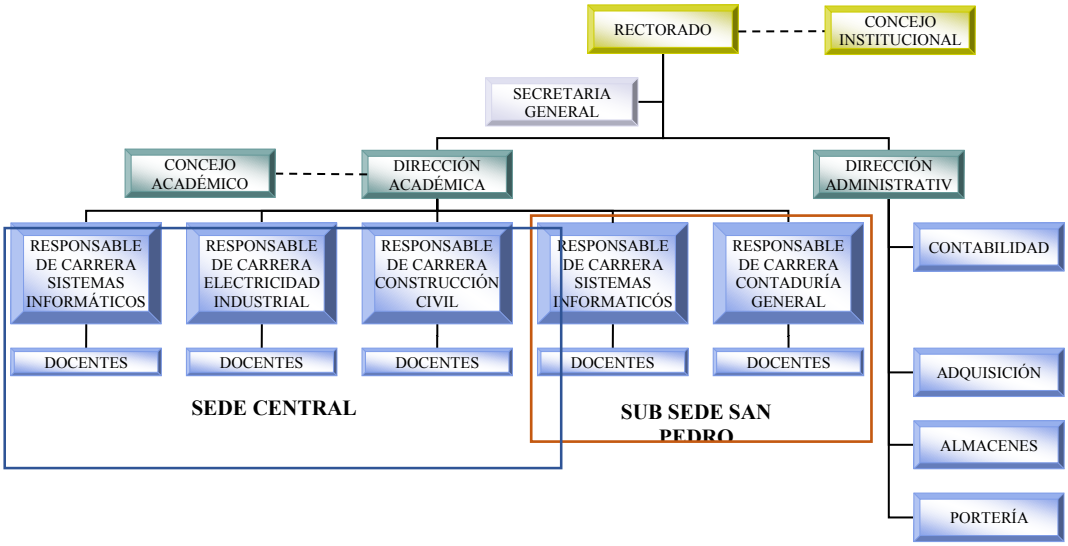
Figura 2. 2: Instituto Tecnológico Marcelo Quiroga Santa Cruz

Fuente: Elaboración propia

2.2.3. ESTRUCTURA ADMINISTRATIVA

El Instituto Tecnológico Marcelo Quiroga Santa Cruz está organizado de la siguiente manera (ver figura 2.3)

Figura 2. 3: Estructura Organizacional



Fuente: Elaboración propia

2.3. MISIÓN Y VISIÓN DE LA EMPRESA

2.3.1. MISIÓN

La Misión del Instituto Tecnológico Marcelo Quiroga Santa Cruz es formar y capacitar profesionales íntegros, éticos, críticos-reflexivos y competitivos, además de implementar programas de certificación sin tomar en cuenta el límite de edad, color, religión, genero u otra situación social, comprometidos con el desarrollo económico, político, social y cultural de su comunidad y con el uso sostenible de los recursos naturales, a través de carreras industriales y comerciales a nivel técnico superior, cursos de capacitación y especialización en beneficio del bien común y de su entorno en general.

2.3.2. VISIÓN

La Visión del Instituto Tecnológico Marcelo Quiroga Santa Cruz se constituye en una institución de formación profesional de alto nivel competitivo y productivo, ofreciendo carreras de educación técnica superior de acuerdo con las demandas de la sociedad, en áreas industriales y comerciales, superando viejas dicotomías, para ofrecer una educación inclusiva e integral, donde los estudiantes puedan satisfacer sus expectativas y demandas del mundo actual y necesidades de la futura sociedad, como pilar fundamental para la construcción del "vivir bien".

2.4. ACTIVIDADES

Actualmente el Instituto Marcelo Quiroga Santa Cruz, tiene una red de datos en diferentes ambientes de la institución con un acceso a internet (ver figura 2.4), así como también darles un mejor servicio a los estudiantes, por lo cual de esta manera accediendo y transmitiendo datos con mucha mayor facilidad, como también mejorar la calidad de servicio que ofrece la institución.

A continuación, se tiene los siguientes activos:

Tabla 2. 1: Hardware de Equipos de Computación

AREA	N.º PC'S	RAM	PROCESADOR	DISCO DURO
ADMINISTRACION	03	8 GB	Inter Corei5 2.8Ghz,	500 GB
LABORATORIO SIS1	15	4 GB, 8 GB	Inter Corei3 2.6Ghz, Inter Corei5 2.8Ghz,	500 GB
LABORATORIO SIS 2	13	2 GB	Inter Core Dos Duo	500 GB
LABORATORIO SIS 3	15	4 GB	Inter Corei5 2.8Ghz,	500 GB
LABORATORIO CONSTRUCCION CIVIL 4	10	8 GB	Inter Corei5 2.8Ghz,	500 GB

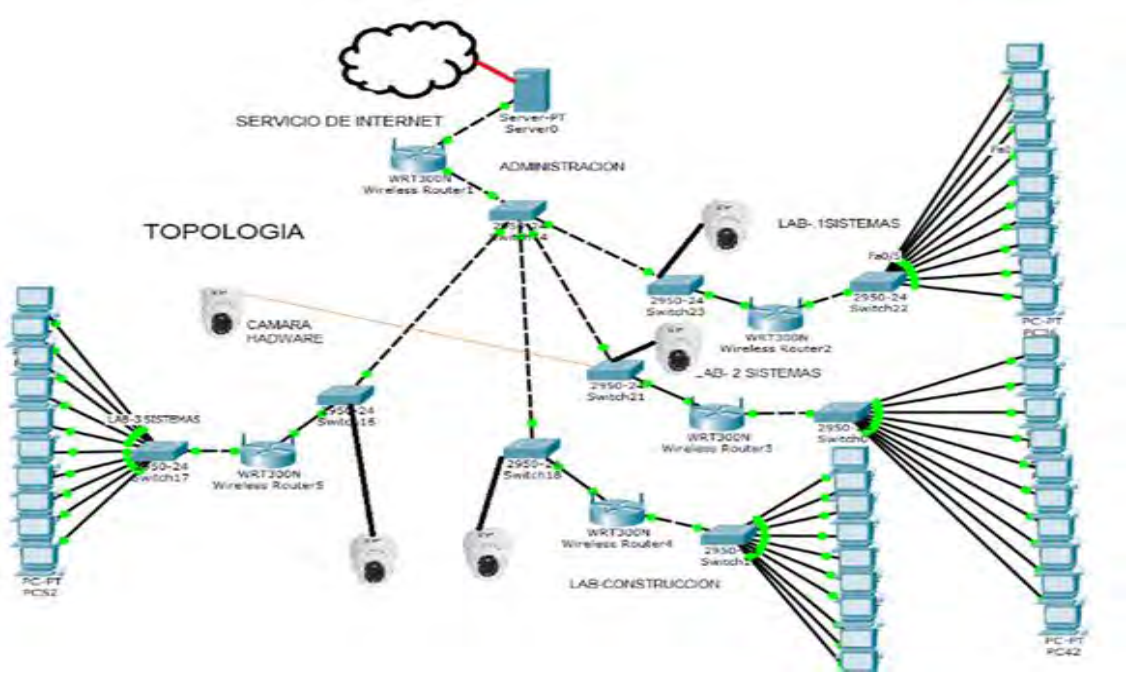
Fuente: Elaboración propia

Tabla 2. 2: Software de Equipos de Computación

AREA	SISTEMA OPERATIVO	APLICACION
ADMINISTRACION	WINDOW 10	Office, Antivirus, otros
LABORATORIO SIS 1	WINDOW 7	Office, programas de programación entre otros
LABOARATORIO SIS 2	WINDOW 7	Office, programas de programación entre otros
LABORATORIO SIS 3	WINDOW 7	Office, programas de programación entre otros
LABORATORIO CC. 4	WINDOW 7	Office, AutoCAD entre otros

Fuente: Elaboración propia

Figura 2. 4: Topología de la Infraestructura de Red



Fuente: Elaboración propia

EQUIPOS DE COMUNICACIÓN (RED)

Tabla 2. 3: Área Administrativa

ITEM	EQUIPO	CANTIDAD	MARCA
1	Switch de 16 puertos rackeable	1	TP-LINK
2	Router- Acher C20	1	TP-LINK
3	Gabinete 5u	1	DLUX
4	PDU- 6 Puertos	1	DLUX
5	Pach panel 24 Puertos	1	SIEMON
6	NVR de 16 canales marca Dahua y disco integrado 4 TB.	1	DAHUA
7	Maus (Negro)	1	DAHUA

Fuente: Elaboración propia

Tabla 2. 4: Laboratorio 1 – Sistemas Informáticos

ÍTEM	EQUIPO	CANTIDAD	MARCA
1	Switch De 24 Puertos Rackeable	1	TP-LINK
2	Mini Rack – Rouland	1	ROULAND
3	Pach-Panel de 24 Puertos	1	SIEMON
4	PDU- 6 Puertos	1	DLUX
5	Router inalámbricos	1	TP – LINK
6	Cámara Seguridad- IP	1	Dahua-alta resolución. 2MP

Fuente: Elaboración propia

Tabla 2. 5: Laboratorio 2 – Sistemas Informáticos

ITEM	EQUIPO	CANTIDAD	MARCA
1	Switch de 24 Puertos- Rackeable	1	TP-LINK
2	Rack Grande	1	ROULAND
3	Pach-Panel de 24 Puertos	1	SIEMON
4	PDU- 8 Puertos	1	SIEMON
5	Estabilizador	1	OMEGA
5	Router inalámbricos	1	TP – LINK
6	Cámara Seguridad- IP	1	Dahua-alta resolución. 2MP

Fuente: Elaboración propia

Tabla 2. 6: Laboratorio 3 – Sistemas Informáticos

ÍTEM	EQUIPO	CANTIDAD	MARCA
1	Switch de 24 puertos- rackeable	1	TP-LINK

2	Rack gabinete grande	1	ROULAND
3	Pach-panel de 24 puertos	1	SIEMON
4	PDF- 6 puertos	1	SIEMON
5	Estabilizador	1	OMEGA
5	Router inalámbricos	1	TP – LINK
6	Cámara Seguridad- IP	1	Dahua-alta resolución. 2MP

Fuente: Elaboración propia

Tabla 2. 7: Laboratorio 4 – Construcción Civil

ÍTEM	EQUIPO	CANTIDAD	MARCA
1	Switch de 24 puertos-rackeable	1	TP-LINK
2	Rack gabinete grande	1	ROULAND
3	Pach-panel de 24 puertos	1	SIEMON
4	PDF- 6 puertos	1	SIEMON
5	Estabilizador	1	OMEGA
5	Router inalámbricos	1	TP – LINK
6	Cámara Seguridad- IP	1	Dahua-alta resolución. 2MP

Fuente: Elaboración propia

Tabla 2. 8: Laboratorio de Hardware – Sistemas Informáticos

ÍTEM	EQUIPO	CANTIDAD	MARCA
1	Cuenta con dispositivos y accesorios de computación.		
1	Cámara Seguridad- IP Dahua-alta resolución. 2MP		

Fuente: Elaboración propia

Tabla 2. 9: Sistema Web para Inscripciones, Registro y control de Notas

DETALLE	CARACTERISTICAS
Lenguajes para el Diseño y Animación Frond End	HTML, CSS, JavaScript
Lenguajes de programación para el Back End	PHP
Gestor de Base de Datos	MySql
URL	http://instec-mqsc.edu.bo/
Dominio	instec-mqsc.edu.bo
Dirección IP	162.222.227.215
Servidores	ns2.bh-34.webhostbox.net ns1.bh-34.webhostbox.net
Proveedor de Hosting	Logic Boxes

Fuente: Elaboración propia

2.4.1. ACTIVIDADES INHERENTES A TI

HARDWARE

Actividad 1: No se realiza un mantenimiento y soporte técnico de los Equipos de Computación y Comunicación, lo cual puede provocar una función inadecuada de los mimos.

Actividad 2: No se cuenta con un generador de energía eléctrica en caso de apagones, y cortes eléctricos.

Actividad 3: No existe un espacio específico donde se tenga almacenada toda la infraestructura de red central, por lo cual cada equipo de comunicación esta expuesta a que cualquier persona que pueda manipularla y acceder fácilmente a la red.

Actividad 4: No se realiza un mantenimiento de los dispositivos instalados de seguridad electrónica de cada laboratorio para su buen funcionamiento.

Actividad 5: En la subsede de San Pedro no se tiene equipos de seguridad como cámaras de vigilancia para salvaguardar los activos.

SOFTWARE

Actividad 1: Los sistemas operativos del área administrativa, no se tiene una contraseña configurada para poder acceder de manera segura a la misma, lo que podría ser vulnerada y acceder fácilmente a la toda la información valiosa de esta institución.

Actividad 2: Se tiene un Sistema Web lo cual realiza todo el registro de las inscripciones, centralizador de notas y generación de boletines bimestrales, trimestrales y anuales, lo cual cada uno de los usuarios tienen como asignado por defecto un usuario que es el número del carnet de identidad y una contraseña que son los primeros 3 dígitos del Carnet de identidad, lo cual es muy vulnerable ya que cualquier persona que sepa el número de carnet de identidad puede ingresar fácilmente al sistema web y modificar o incluso borra datos muy importantes.

Actividad 3: La información almacenada en la base de datos del sistema web, no se realiza una copia de respaldo de la información (backup), lo cual si existiera un ataque cibernético podría perder toda la información y generaría una catástrofe a la institución.

Actividad 4: No existe un manteniendo y soporte del sistema web.

Actividad 5: La configuración de los routers tp-link no es la adecuada ya que si alguien con solo conectar un equipo a la red podría realizar un ataque Man In The Middle (Hombre en el Medio), envenenamiento de la red, propagación de virus informático y entre otros.

RECURSOS HUMANOS

Actividad 1: No existe un responsable para el monitoreo y control de los sistemas y dispositivos de comunicación.

Actividad 2: No existe un Reglamento que defina cual debería ser el proceso para la buena administración de la Tecnología de la Información y Comunicación (TIC).

Actividad 3: No existe una capacitación hacia los usuarios a cerca como deberían de manejar adecuadamente estas Tecnologías de la Información (TI).

Actividad 4: Las contraseñas de la parte administrativa al momento de realizar la inscripción se accede con el usuario administrador que en este caso es el usuario de secretaria general

por lo cual como cada docente necesita ingresar al sistema con ese usuario administrador para poder realizar la inscripción de los estudiantes se lo proporciona en una hoja que esta pegada en la PC y que si alguna persona (estudiante, docente u otra persona ajena) pueda ver o memorizar ese tipo de usuario administrador, podría fácilmente acceder al sistema web y manipular todo el sistema lo cual podría ocurrir un borrado total de la información almacenada.

Actividad 5: La información que el área administrativa (Rectorado, Dirección Académica, Dirección Administrativa y Secretaria General) tiene almacenada en su equipo de computación, no realiza una copia de respaldo de esa información, ni tampoco se tiene una adecuada organización de los mismos, lo cual genera que esa información cuando se lo necesite no se lo tenga disponible inmediatamente y genera demora en el trabajo eficiente del mismo

CAPITULO III

MARCO TEÓRICO

CAPÍTULO III

MARCO TEÓRICO

Este capítulo constituye una de las secciones más importantes de la propuesta de trabajo final, ya que contiene las teorías en la que se sustenta el proyecto planteado.

Por nuestra condición de país en vías de desarrollo, somos dados a importar posiblemente tecnología ya desechada en otros países y que no se adapta a nuestro medio. El conjunto de referencias teóricas coadyuvará a sustentar la propuesta.

La gestión integral de los riesgos es un proceso estructurado, consistente y continúo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos.

Los procesos de gestión de riesgos en organizaciones no complejas son distintos a los que se utilizan en las organizaciones de mayor complejidad. Sin embargo, no hay normas estrictas que dicten cómo debe una entidad manejar el proceso. Su grado de rigor debe cumplir con los dictados de la alta dirección, y ser apropiado en función de los riesgos en cuestión.

El presente capítulo, pretende mostrar la referencia teórica relacionada a aspectos fundamentales de sistemas de información, tecnología de la información, gobierno y gestión, ISO 27000, ISO 20000, ISO 38500, COBIT 5, COSO, ITIL V3 y BS 25999; para luego, proponer un modelo de gestión de Riesgos de TI bajo el enfoque de Cobit 5, con la finalidad de promover un gobierno de TI y, por ende, de esta manera, lograr una mejor gestión del riesgo al que pueden estar expuestas hoy en día las empresas.

3.1. SISTEMA DE INFORMACIÓN

Conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de

control en una organización (Laudon, 2010). El objetivo consiste en: proveer la información necesaria (pasada, presente y futura) en forma precisa y oportuna para una correcta toma de decisiones.

Los SI contienen información sobre personas, lugares y cosas importantes dentro de la organización, o en el entorno que la rodea. Por información nos referimos a los datos que se han modelado en una forma significativa y útil para los seres humanos. Por el contrario, los datos son expresiones simbólicas, que por sí mismas no tienen sentido semántico.

Existen diferentes sistemas de información en la empresa: Sistemas de Procesamiento de Transacciones (TPS), Sistemas del Trabajo del Conocimiento (WKS), Sistemas de Información Gerencial (MIS), Sistemas de Soporte a Decisiones (DSS), Sistemas de Inteligencia de Negocios (BIS), Sistemas de Apoyo a Ejecutivos (ESS), Sistemas de Planificación de Recursos Empresariales (ERP), Sistemas de la Cadena de Suministros (SCM), Sistemas de las relaciones con los clientes (CRM), entre los más importantes.

3.2. TECNOLOGÍA DE LA INFORMACIÓN (TI)

La TI es una de las diversas herramientas que utilizan los directores para lidiar con el cambio. El hardware de computadora es una máquina compuesto por elementos físicos, de origen electrónico, capaz de realizar una variedad de trabajos a gran velocidad y con gran precisión siempre y cuando se le de las instrucciones necesarias (adecuadas). Consiste en: computadoras de diversos tamaños y formas (incluyendo los dispositivos móviles de bolsillo); varios dispositivos de entrada, salida y almacenamiento; y dispositivos de telecomunicaciones que conectan a las computadoras entre sí.

El software de computadora es una producción inmaterial producto del cerebro humano. Consiste en las instrucciones detalladas y pre-programadas que controlan y coordinan los componentes de hardware de computadora en un sistema de información.

La tecnología de almacenamiento de datos consiste en el software que gobierna la organización de los datos en medios de almacenamiento físico.

La tecnología de redes y telecomunicaciones, que consiste tanto de los dispositivos físicos como de software, conecta las diversas piezas de hardware y transfiere datos de una ubicación física a otra. Las computadoras y el equipo de comunicaciones se pueden conectar en redes para compartir voz, datos, imágenes, sonido y video. Una red enlaza a dos o más computadoras para compartir datos o recursos, como una impresora. La red más grande y utilizada del mundo es Internet: una "red de redes" global que utiliza estándares universales para conectar millones de redes distintas. Internet creó una nueva plataforma de tecnología "universal", sobre la cual se pueden crear nuevos productos, servicios, estrategias y modelos de negocios. Esta misma plataforma tecnológica tiene usos internos, pues provee la conectividad para enlazar los distintos sistemas y redes dentro de una empresa. Las redes corporativas internas basadas en tecnología de Internet se denominan intranets. Las intranets privadas que se extienden a los usuarios autorizados fuera de la organización se denominan extranets; las empresas usan dichas redes para coordinar sus actividades con otras empresas para realizar compras, colaborar en el diseño y otros tipos de trabajo interno a la organización. Para la mayoría de las empresas en la actualidad, utilizar tecnología de Internet es tanto una necesidad de negocios como una ventaja competitiva. World Wide Web es un servicio proporcionado por Internet, que utiliza estándares aceptados en forma universal para almacenar, recuperar y mostrar información en un formato de página en Internet. Las páginas Web contienen gráficos, animaciones, sonidos y video, y están enlazadas con otras páginas Web. Al hacer clic en palabras resaltadas o botones en una página Web, usted puede enlazarse con las páginas relacionadas para encontrar información adicional y enlaces o vínculos hacia otras ubicaciones en Web.

Todas estas tecnologías, junto con las personas requeridas para operarlas y administrarlas, representan recursos que se pueden compartir en toda la organización y constituyen la infraestructura de tecnología de la información (TI) de la empresa. La infraestructura de TI

provee la base, o plataforma, sobre la que una empresa puede crear sus sistemas de información específicos. Cada organización debe diseñar y administrar con cuidado su infraestructura de TI, de modo que cuente con el conjunto de servicios tecnológicos que necesita para el trabajo que desea realizar con los sistemas de información.

3.3. GOBIERNO Y GESTIÓN

El concepto de gobierno y gestión de riesgos de TIC surge a partir de la noción de gobierno y gestión de TIC.

3.3.1. ¿QUÉ ENTENDEMOS POR GOBIERNO?

El gobierno asegura, según (Braga, 2015), que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

El Gobierno según (Muñoz & Martinez, 2012), asegura que las necesidades de los *Stakeholders (interesados)*, condiciones y opciones sean evaluadas para determinar un balance en el logro de los objetivos estratégicos de la organización, con el propósito de establecer una clara dirección de la organización a través de procesos de priorización y toma de decisiones; y monitorear su desempeño y cumplimiento cotejándolo con los objetivos establecidos por la dirección.

Entendido el gobierno de TI, tal como lo establece el estándar internacional ISO/IEC 38500:2008 como un sistema por el que se dirige y controla la utilización actual y futura de las TIC.

En coherencia con lo expuesto, el gobierno de riesgos de TIC, es el sistema por el cual se dirigen y controlan las incertidumbres presentes y futuras que generan las tecnologías de información en la organización.

3.3.2. ¿QUÉ ENTENDEMOS POR GESTIÓN?

La gestión planifica, construye, ejecuta y supervisa actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

La Gestión según (Muñoz & Martinez, 2012), posibilita la planeación, construcción, ejecución y monitoreo de actividades alineadas con la dirección; establecidas por el gobierno, para alcanzar los objetivos estratégicos de la organización.

En la mayoría de las organizaciones, la gestión es responsabilidad de la dirección ejecutiva bajo el mando del CEO[3].

La gestión de TI, se centra en administrar e implementar la estrategia tecnológica del día a día, y su enfoque está más orientado al suministro interno de TI, definido de igual forma por la norma internacional como el sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización, y está sujeta a la guía y monitoreo del gobierno de TI.

La gestión de riesgos de TIC se centra en los procesos requeridos para garantizar niveles aceptables de riesgo de la información y de la infraestructura tecnológica incorporada en el día a día del negocio.

[3] CEO (Chief Executive Officer). Consejero delegado o director ejecutivo, es el máximo responsable de la gestión y dirección administrativa de la empresa.

3.4. RIESGO

El riesgo puede definirse como aquella eventualidad que imposibilita el cumplimiento de un objetivo, es una circunstancia el cual se está siempre expuesto sea cual tipo de riesgo que se asocie según la actividad. El riesgo es la probabilidad que un peligro (causa inminente de pérdida), existente en una actividad determinada durante un período definido, ocasione un incidente de ocurrencia incierta pero con consecuencias factibles de ser estimadas.

Podemos definirla también, como el efecto de la incertidumbre en la consecución de los objetivos:

1) Incertidumbre (puede que nunca ocurra).
2) El riesgo importa y debe gestionarse porque tiene un efecto (positivo y negativo).
3) Ese efecto es sobre los objetivos fijados.

El riesgo se puede catalogar de dos tipos, inherente y residual, se entiende por inherente aquel que surge como exposición que se tenga sobre la actividad en particular, este tipo de riesgo es propio, entiéndase como aquel que siempre estará presente y no puede ser eliminado, como ejemplo, el salir al destino de trabajo, requerir transporte y presentarse un volcamiento; por otro lado el riesgo residual es aquel que continua manifestándose una vez se apliquen controles y /o acciones para mitigarlo mediante posibles estrategias, gestiones y criterios para aminorar el riesgo inherente.

Vale la pena esclarecer que el riesgo siempre conllevará a dos efectos, ya sea a una pérdida o a una ganancia; en lo referente con la tecnología, de acuerdo con el objetivo del siguiente estudio, el riesgo se plantea como amenaza, como, por ejemplo, el riesgo a perder datos debido a una deficiencia de la plataforma, un virus informático, e inclusive mal funcionamiento de la red entre otros.

Por todo lo anterior para las organizaciones es imprescindible identificar aquellos riesgos relevantes a los cuales se pueda ver enfrentado y que conlleven un peligro para la consecución de sus objetivos, más aún cuando la rentabilidad de su negocio está íntimamente ligada a dichos riesgos.

La identificación de estos riesgos es un proceso iterativo y generalmente integrado a la estrategia y planificación y su análisis se relaciona con la criticidad del proceso o actividad y con la importancia del objetivo, más allá que éste sea explícito o implícito.

Una vez que los riesgos han sido identificados a nivel del organismo, deberá practicarse similar proceso a nivel de programa y actividad. Se considerará, en consecuencia, un campo más limitado, enfocado a los componentes de las áreas y objetivos claves identificadas en el análisis global del organismo.

Podemos mencionar, al respecto que en el caso de entidades financieras se requiere identificar, valorar y cuantificar su exposición al riesgo, optimizando al mismo tiempo la rentabilidad, que se traslada directamente al cliente mediante unos precios más competitivos y la generación de mayores beneficios.

3.4.1. TIPOS DE RIESGO

3.4.1.1.RIESGO TECNOLÓGICO

El riesgo tecnológico es la probabilidad de que un objeto, material o proceso ocasione un número determinado de consecuencias a la economía, salud, medio ambiente y/o desarrollo integral de un sistema.

Si bien es cierto que la tendencia dominante es la de asociar los eventos naturales como elementos desencadenantes de desastres, cada vez surgen más elementos que invitan a

considerar los riesgos tecnológicos como un elemento que debe ser considerado en cualquier iniciativa destinada a la gestión integral del riesgo de desastres en espacios urbanos y rurales.

Los riesgos tecnológicos pueden presentarse en una amplia gama de variedades, debe tenerse presente que no hay dos accidentes idénticos. Según la variedad de la amenaza, pueden ser:

- Riesgo por Incendio o explosión;
- Riesgo por escapes o derrames;
- Riesgo de intoxicación y exposición a radiaciones ionizantes.

La amenaza tecnológica se enmarca en el contexto de las amenazas de origen antropogénico (por la acción del hombre).

La otra generalidad de las amenazas de este tipo son las denominadas "Antrópico-tecnológicas" se derivan de la existencia y manejo inadecuado de instalaciones industriales complejas u otras actividades que puedan generar un factor de inseguridad a la población.

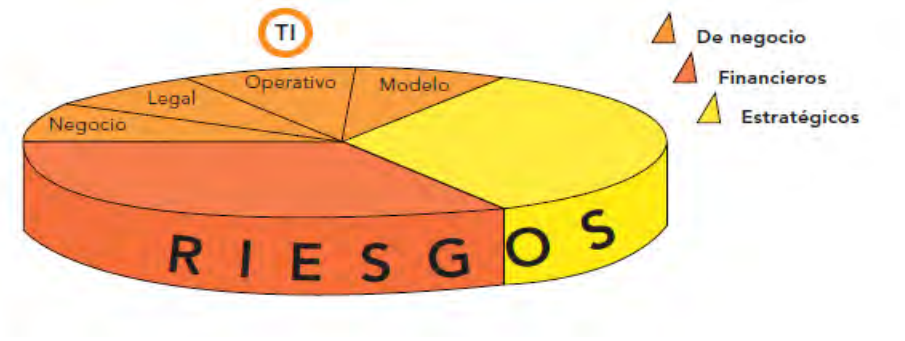
La vulnerabilidad, se define como el grado de exposición de un sistema a los efectos de la amenaza y está determinada por la insuficiencia que tenga ese sistema, un sujeto o una comunidad, para hacer frente al cambio que produce un accidente tecnológico.

Un riesgo tecnológico o informático se refiere a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los productos o servicios informáticos como por ejemplo los equipos informáticos, instalaciones, proyectos, programas (softwares incorporados), datos confidenciales entre otros.

Las amenazas y vulnerabilidades son ciertas acciones que ocasionan consecuencias negativas en la operación de la empresa. Estos dos conceptos son importantes puesto que, al optar por usar un nuevo software para optimizar un proceso dentro de la empresa, éste puede ser vulnerable a incurrir en fallas, e incluso a un uso inadecuado del mismo.

El riesgo tecnológico no se conforma necesariamente en el área de Tecnología de información (TI), aunque esta brinde soporte a las diversas áreas del Grupo y sea fundamental dentro de las estrategias de negocio de una organización, no es en dicha área en donde se materialice el riesgo necesariamente. Para un entendimiento adecuado sobre la relación del riesgo tecnológico con la empresa, se debe considerar el flujo existente o vínculos directos entre los componentes de la tecnología, los procesos, el logro de objetivos, el cumplimiento de metas y hasta la satisfacción de los *stakeholders*. (ver figura 3.1). Se debe de tener claro que el riesgo siempre estará presente en todas las áreas de la organización.

Figura 3. 1: El Riesgo



Fuente: Gustavo A. Solís Montes, (CobiT User Convention-CobiT y la administración de riesgos).

3.4.1.1.1. PÉRDIDA ESPERADA

Es una medida de riesgo entendida como el producto entre la probabilidad e incumplimiento y el porcentaje de pérdida producida por dicho incumplimiento. Es un costo del negocio, que refleja lo que realmente se espera perder en promedio (valor medio de las pérdidas). Existe una relación inversa entre la probabilidad de incumplimiento de un título calificado y su calificación, es decir que ante una mayor probabilidad de incumplimiento, menor es la calificación del título. El tiempo es otro factor que entra en la relación entre probabilidades de incumplimiento y calificaciones: ante un mayor tiempo de circulación del título calificado, mayor la probabilidad de incumplimiento, dado un nivel específico de calificación

3.4.1.1.2. PÉRDIDA INESPERADA

Es una medida de riesgo (volatilidad de pérdidas) que surge como consecuencia de que las pérdidas reales que pueda tener una organización sean superiores a las esperadas. Podemos realizar una distinción entre pérdida inesperada de carácter reversible, donde en un momento determinado el precio de mercado de un título puede caer, pero con el tiempo puede recuperarse, por el contrario tenemos aquellas pérdidas inesperadas e irreversibles, en las cuales no existe posibilidad de recuperación

3.4.1.2.RIESGO CREDITICIO

El riesgo de crédito también llamado riesgo de solvencia o fallo, es usual de las entidades financieras, por estar vinculado a la operativa de estas entidades y presente en todas sus operaciones de activo. Este señala la posibilidad de incurrir en pérdidas como consecuencia del incumplimiento, total o parcial, por parte del acreditado, de los recursos prestados o avalados en una operación financiera al vencimiento de los pagos o retornos pactados, ya sea por incapacidad de éste o por falta de disposición, en tiempo o en forma. O también a los efectos que produciría el deterioro de la calidad de crédito del acreditado.

El riesgo de Crédito puede analizarse de tres dimensiones básicas:

1. Riesgo de Incumplimiento;
2. Riesgo de Exposición;
3. Riesgo de Recuperación.

3.4.1.3.RIESGO FINANCIERO

El riesgo Financiero es un riesgo inherente a la realización de operaciones financieras debido a la incertidumbre que existe al momento de ser realizadas. Podemos también decir que es el riesgo de no estar en condiciones de cubrir los costos financieros, por esto su análisis se puede

determinar por el grado de apalancamiento financiero que posea la organización en un momento determinado. El cual engloba consecuencias adversas que puedan producirse por una alteración cuantitativa o cualitativa en los ingresos presupuestarios, recogiendo las disminuciones efectivas de recursos financieros mantenidos en ejercicios presupuestarios previos, así como el desaprovechamiento de iniciativas que faciliten el incremento o diversificación de las fuentes de financiación.

El riesgo financiero está compuesto por:

1. Riesgo de tasa de interés;
2. Riesgo cambiario;
3. Riesgo de liquidez.

3.4.1.4.RIESGO DE OPERACIONES

El riesgo operacional surge de la posibilidad que una organización incurra en pérdidas inesperadas, directas e indirectas, como consecuencia de sistemas de control de gestión inadecuados, problemas operativos, incumplimiento de controles internos, fraudes, problemas imprevistos o bien acontecimientos externos que no permiten asegurar la integridad, efectividad y eficiencia de las operaciones.

Este riesgo comprende: desarrollo y oferta de productos, procesamiento de la operación, desarrollo de sistemas, sistemas computarizados, complejidad de los productos y servicios, y el entorno de control interno.
Entre sus objetivos se encuentran identificar los riesgos, monitorear que los mismos se mitigan a niveles aceptables y cuantificar su consumo de capital. Es así como sus responsabilidades no incluyen la reingeniería de procesos u optimización.

La gestión de este riesgo es una temática de creciente sensibilidad para las empresas de cualquier sector económico y en particular para la industria bancaria. La necesidad de

identificar los peligros y gestionarlos adecuadamente es clave en la realización de dicho negocio.

3.5. ANÁLISIS Y GESTIÓN DE RIESGOS

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

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

Los objetivos, estrategias y políticas generales de seguridad de la organización, son elementos base para la seguridad de TI. Estos proporcionan soporte a la actividad de la organización y aseguran la consistencia entre todas las salvaguardas.

El primer paso, descrito en el párrafo anterior, sirve para comenzar con el análisis y gestión de riesgos. El análisis y gestión de riesgos es uno de los elementos claves de todo proceso de gestión de la seguridad informática.

Se identifican dos procesos:

1) Análisis de riesgo, permite la identificación de las amenazas que acechan a los distintos activos del sistema para determinar la vulnerabilidad del mismo ante esas amenazas y para estimar el impacto que una seguridad insuficiente puede tener para

la organización conociendo, por tanto, el riesgo que corre [ARIA 2005]. Conlleva el análisis de los activos, amenazas y vulnerabilidades valorándose los riesgos en términos de impacto potencial que podría ser causado por la pérdida de confidencialidad, integridad y disponibilidad de la información y recursos del sistema.

2) Gestión de riesgos, que, basándose en el análisis de riesgos, permite seleccionar las medidas o salvaguardas de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles impactos [ARIAS 2005].

El análisis de riesgos de un Sistema de Información (SI) tiene por objeto identificar los riesgos, las amenazas y vulnerabilidades existentes determinando su magnitud, mostrando la situación de la seguridad presente en una organización respecto al procesado, transmisión y almacenamiento de la información, y como consecuencia reuniendo los hechos básicos necesarios para seleccionar las contramedidas y los procedimientos adecuados para minimizar las amenazas y las vulnerabilidades.

Un riesgo de seguridad se puede definir como la probabilidad de que una vulnerabilidad de un sistema o red sea explotada por una amenaza, comprometiendo de esta forma al sistema o su información. Debido al carácter cambiante de las amenazas, un análisis de riesgos debe ser actualizado periódicamente. Todo SI tiene unos riesgos inherentes al mismo.

El análisis de riesgos permite establecer los riesgos que existen y, a partir de ahí, establecer los requisitos de seguridad necesarios para prevenir una determinada situación, contener su efecto, o simplemente reconocer que existe un riesgo potencial de pérdida de datos. Por ello el análisis de riesgos es necesario y recomendable en todo sistema o red, ayudando a identificarlos, así como en la toma de decisiones a adoptar para eliminar el riesgo, minimizarlo o asumirlo, pero con el conocimiento de su existencia, riegos e impacto.

3.5.1. ASPECTOS A CONSIDERAR EN LA GESTIÓN DE RIESGOS

- Criterios en seguridad de la información:
  - **Confidencialidad:** Es un término asociado con el acceso y uso de la información solo por parte de quienes se encuentran autorizados y tienen la necesidad de conocerla. En términos formales, y de acuerdo a lo establecido en la norma ISO/IEC 27000, la confidencialidad es la propiedad que tiene la información de no estar disponible o revelada a individuos, entidades o procesos no autorizados.

    El concepto de confidencialidad es más cercano a la información que a los activos tecnológicos y persigue fundamentalmente que esta sea accesible únicamente por las personas, entidades o mecanismos autorizados.

    La confidencialidad está asociada con secretos de diversa índole (personales, empresariales, militares), algunos de ellos son técnicos, como la descripción de un método de fabricación (ejemplo, la fórmula de la CocaCola), otros son de índole comercial como una lista de nombres y direcciones de clientes que podría interesar a un competidor, e incluso militares, como planes de guerra, o planes de incursión.

    Dentro de los casos más sonados a nivel internacional que se encuentran relacionados con la Confidencialidad está el caso de Wikileaks, una plataforma digital para compartir documentos, que se hizo famosa desde julio de 2010 debido a los miles de documentos de carácter reservado que ha difundido por la web, ganándose la antipatía del gobierno de los Estados Unidos, al divulgar más de 251 mil cables diplomáticos de sus embajadas en 274 países.
  - **Integridad:** Es un concepto que presenta diversas interpretaciones, en general podría definirse como la propiedad de salvaguardar la exactitud e integridad de la información y de los activos tecnológicos, ante su modificación o destrucción no autorizada.

    De acuerdo con COBIT, la integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a las expectativas y valores del negocio.

La ISO/IEC 27000: 2014 define la integridad de la información como la propiedad de exactitud y completitud. Si la información está completa y libre de errores, es integra.

- **Disponibilidad:** Referido a que los usuarios autorizados tienen acceso a la información y a los activos tecnológicos, cuando lo requieran. Para COBIT la disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento.

  La ISO/IEC 27000:2014 define la disponibilidad como la propiedad de ser accesible y utilizable a petición de una entidad autorizada.

  Dentro de las amenazas más cotidianas que afectan la disponibilidad de la información y/o de los activos tecnológicos se encuentra la denegación de servicio. La disponibilidad de la información y/o de los activos tecnológicos asociados se puede presentar de forma cotidiana en diversas formas, algunos ejemplos de ellas son: La salida de un sistema de información bancario de atención al cliente, ante problemas de bases de datos; un servidor crítico fuera de línea ante un corte de energía; imposibilidad de acceder a la información de un computador personal por problemas de hardware o por una falla del sistema operativo o por caídas de red.

- Elementos a considerar (las cuatro P's) para un sistema de gestión de la seguridad de la información efectivo:
  - Procesos: Gestión de riesgos y Manejo de incidentes
  - Personas: Entrenamiento, Educación y certificaciones;
  - Productos y tecnologías; Firewalls, antivirus, anti spyeare, redes;
  - Proveedores

3.5.2. GESTIÓN INTEGRAL DEL RIESGO

Gestionar el riesgo es pensar hacia el futuro. Es encontrar un equilibrio entre los costos y los beneficios de la empresa. La Gestión Integral de Riesgo consiste en detectar oportunamente

los riesgos que pueden afectar a la empresa para generar estrategias que se anticipen a ellos y los conviertan en oportunidades de rentabilidad para la empresa.

Los líderes de las empresas más exitosas de la actualidad no asumen los riesgos; los estudian y modelan para gestionarlos (ver figura 3.2) y sacarles todo el partido, es decir: los convierten en aumento de rentabilidad para la empresa. Estas empresas trabajan continuamente para optimizarlos y transformarlos en oportunidades que las ayuden a avanzar en su camino hacia el crecimiento, por lo tanto, son empresas más rentables y con niveles de riesgos aceptables para la dirección. La Gestión Integral de Riesgo permite anticiparse al mismo y asegurar los objetivos y metas estratégicas definidas por la empresa u organización.

Figura 3. 2: Riesgos relacionados con TI

Fuente: Grant Thornton Argentina

3.6. GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

Dentro de los modelos de gestión de TI soportados bajo el enfoque de procesos y gestión de riesgos, se encuentran las normas:

ISO 27000;
ISO 31000;
COBIT 5;
COSO;
ITIL;
BS 25999

Cuya implementación debe asegurar un trabajo eficiente y orientado con las directrices estratégicas de las diferentes instituciones. La consideración simultanea de estos modelos de gestión, requiere de un proceso sincronizado de implementación que evite la duplicidad de operaciones y las estructuras burocráticas a nivel documental, de tal manera que se configure un verdadero sistema integrado de gestión alrededor de los servicios de TI. Los lineamientos básicos como: ISO 27005, ISO 31000, COBIT 5, COSO, ITIL V3 y BS 25999, permitirán seguir una ruta estratégica a las organizaciones para estar mejor preparada ante un entorno cambiante y de alto riesgo.

3.6.1. NTC - ISO 27005

Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo. Esta norma suministra directrices para la gestión del riesgo en la seguridad de la información.

Esta norma brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

3.6.1.1.TÉRMINOS Y DEFINICIONES

- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

- **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Comunicación del riesgo:** Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- **Transferencia del riesgo:** Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

Es necesario un enfoque sistemático para la gestión del riesgo en la seguridad de la información para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información y para crear un sistema de gestión de la seguridad de la información (SGSI) eficaz. Este enfoque debería ser adecuado para el entorno de la organización y, en particular, debería cumplir los lineamientos de toda la gestión del riesgo en la empresa. Los esfuerzos de seguridad deberían abordar los riesgos de una manera eficaz y oportuna donde y cuando sean necesarios. La gestión del riesgo en la seguridad de la información debería ser una parte integral de todas las actividades de gestión de seguridad de la información y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

3.6.1.2.INFORMACIÓN GENERAL

La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo

analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

- La gestión del riesgo en la seguridad de la información debería contribuir a:
- La identificación de los riesgos;
- La evaluación de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia;
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos ;
- El establecimiento del orden de prioridad para el tratamiento de los riesgos;
- La priorización de las acciones para reducir la ocurrencia de los riesgos;
- La participación de los interesados cuando se toman las decisiones sobre gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo;
- La eficacia del monitoreo del tratamiento del riesgo;
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos;
- La captura de información para mejorar el enfoque de la gestión de riesgos;
- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos.

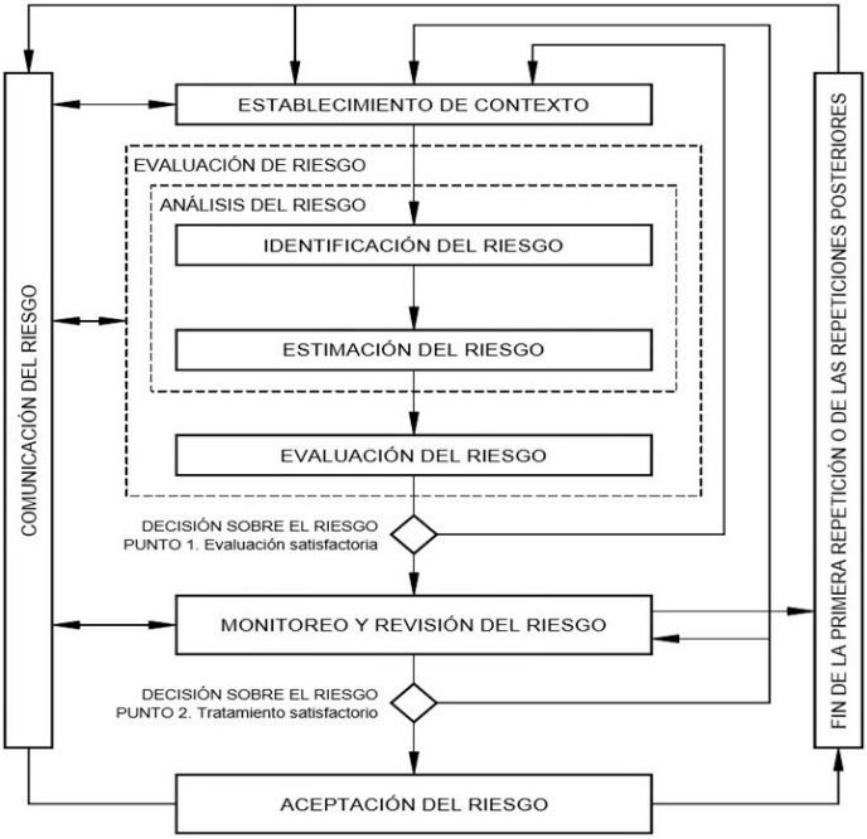
3.6.1.3.VISIÓN GENERAL

El proceso de gestión del riesgo en la seguridad de la información consta del:

- Establecimiento del contexto;
- Evaluación del riesgo;
- Tratamiento del riesgo;
- Aceptación del riesgo;
- Comunicación del riesgo;
- Monitoreo y revisión del riesgo.

La Figura 3.3, muestra el proceso de gestión del riesgo en la seguridad de la información como un proceso iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo.

Figura 3. 3: Proceso de Gestión de Riesgos



Fuente: NTC-ISO/IEC 27005

3.6.2. ISO 31000

3.6.2.1.INTRODUCCIÓN

Esta Norma Internacional puede ser utilizada por cualquier organización, de carácter público, privado, sin fines de lucro, asociación, grupo o individuo, y no es específica a alguna industria o sector.

Cuando la gestión del riesgo se implementa y se mantiene de acuerdo con esta norma ISO 31000, le permite a la organización:

- Aumentar la probabilidad de alcanzar los objetivos;
- Fomentar la gestión proactiva;
- Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización;
- Cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales;
- Mejorar la presentación de informes obligatorios y voluntarios;
- Mejorar el gobierno;
- Mejorar la confianza y honestidad de las partes involucradas,
- Establecer una base confiable para la toma de decisiones y la planificación;
- Mejorar los controles;
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo;
- Mejorar la eficacia y la eficiencia operativa;
- Incrementar el desempeño de la salud y la seguridad, así como la protección ambiental;
- Mejorar la prevención de pérdidas y la gestión de incidentes;
- Minimizar las pérdidas;
- Mejorar el aprendizaje organizacional; y
- Mejorar la flexibilidad organizacional.
- Esta norma está destinada a satisfacer las necesidades de un rango amplio de partes involucradas, incluyendo:

  a) aquellos responsables del desarrollo de la política de gestión del riesgo dentro de la organización;

  b) aquellos responsables de garantizar que el riesgo se gestiona eficazmente dentro de la organización como unidad o dentro de un área, proyecto o actividad específicos;

c) aquellos que necesitan evaluar la eficacia de una organización en cuanto a la gestión del riesgo; y

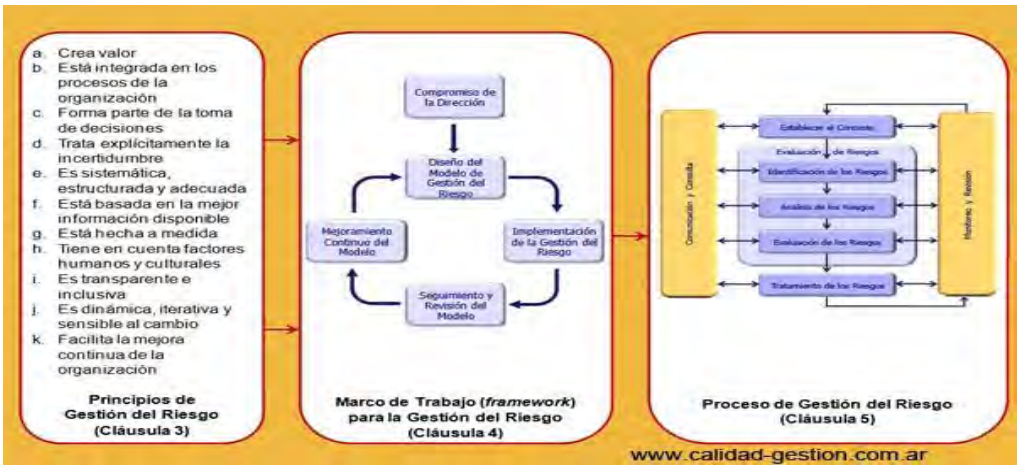
d) aquellos que desarrollan normas, guías, procedimientos y códigos de práctica que, parcial o totalmente, establecen la manera de gestionar el riesgo dentro del contexto específico de estos documentos.

3.6.2.2.PRINCIPIOS BÁSICOS, MARCO DE TRABAJO Y PROCESO

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

La relación entre los Principios Básicos de la Gestión de Riesgos, el Marco de Trabajo (Framework), así como el Proceso de Gestión del Riesgo desarrollado en la Norma ISO 31000 se resume en la figura 3.4 siguiente:

Figura 3. 4: Principios Básicos de la Gestión de Riesgos



Fuente: ISO 31000

Cuando se implementa y mantiene de acuerdo con esta norma internacional, la gestión del riesgo de permite a una organización:

- Aumentar la probabilidad de lograr los objetivos;
- Fomentar la gestión proactiva;
- Ser conscientes de la necesidad de identificar y tratar los riesgos en toda la organización;
- Mejorar la identificación de las oportunidades y amenazas;
- Cumplir con las exigencias legales y reglamentarias y las normas internacionales;
- Mejorar la información obligatoria y voluntaria;
- Mejorar la gobernanza;
- Mejorar la confianza de los interesados y la confianza;
- Establecer una base confiable para la toma de decisiones y la planificación;
- Mejorar los controles;
- Asignar y utilizar eficazmente los recursos para el tratamiento del riesgo;
- Mejorar la eficacia operacional y la eficiencia;
- Mejorar la salud y de seguridad, así como la protección del medio ambiente;
- Mejorar la prevención de pérdidas y gestión de incidentes;
- Minimizar las pérdidas;
- Mejorar el aprendizaje de la organización, y
- Mejorar la resistencia de la organización.

3.6.2.3.ÁMBITO DE APLICACIÓN

Esta norma proporciona principios y directrices de carácter genérico sobre la gestión de riesgos. Puede ser utilizado por cualquier institución pública, privada o empresa de la comunidad, grupo o individuales. Esta norma puede ser aplicada en todo el ciclo de vida de una organización.

3.6.2.4.MARCO DE GESTIÓN DEL RIESGO

Actitud ante el riesgo

Enfoque de la organización para evaluar y, eventualmente, seguir, mantener, adoptar o alejarse de riesgo.

Plan de gestión de riesgos

Régimen en el marco de la gestión del riesgo especificando el planteamiento, la gestión de componentes y los recursos que se aplicarán a la gestión del riesgo

NOTA 1: Los componentes de gestión suelen incluir los procedimientos, prácticas, la asignación de responsabilidades, la secuencia de y el calendario de actividades.
NOTA 2 El plan de gestión de riesgo se puede aplicar a un determinado producto, proceso y proyecto, y parte o la totalidad de la organización.

Proceso de gestión de riesgos

La aplicación sistemática de políticas de gestión, procedimientos y prácticas para las actividades de comunicación, consultoría, se establece el contexto, y la identificación, análisis, evaluación, tratamiento, seguimiento y la revisión de riesgo.

Establecer el contexto

La definición de los parámetros internos y externos que deben tenerse en cuenta en la gestión de riesgos, y el establecimiento del ámbito de aplicación y criterios de riesgo para la política de gestión del riesgo.

Contexto externo

Entorno externo en el que la organización busca alcanzar sus objetivos. Puede incluir: La cultural, social, político, jurídico, reglamentario, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local; Factores clave y las tendencias con repercusiones en los objetivos de la organización, y la relaciones con, y las percepciones.

Contexto interno

Ambiente interno en el que la organización busca alcanzar sus objetivos. Puede incluir:

- Gobernanza, la estructura organizativa, las funciones y responsabilidades;
- Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos;
- La capacidad, entendida en términos de recursos y conocimientos (capital, por ejemplo, tiempo, Personas, procesos, sistemas y tecnologías);
- Los sistemas de información, flujos de información y la toma de decisiones (tanto formales como informales);
- Relaciones con, y las percepciones y los valores de, grupos de interés internos; Cultura de la organización;
- Normas, directrices y modelos adoptados por la organización, y
- La forma y el alcance de las relaciones contractuales.

Comunicación y consulta

Procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir y obtener información y para entablar un diálogo con las partes interesadas en relación con la gestión del riesgo.

Interesados (Stackholder)

Persona u organización que pueden afectar, ser afectados por, o sienten que se encuentran afectados por una decisión o actividad.

La identificación de riesgos

Proceso de encontrar, reconocer y describir los riesgos.

NOTA 1: Identificación de riesgos implica la identificación de las fuentes de riesgo, eventos, sus causas y sus posibles consecuencias.

NOTA 2 de identificación de riesgos puede incluir datos históricos, el análisis teórico, y opiniones de expertos, y de necesidades del Stakeholder.

Fuente de riesgo

Elemento que por sí sola o en combinación tiene el potencial intrínseco para dar lugar a riesgo.

Evento

La aparición o cambio de un conjunto particular de circunstancias

NOTA 1 Un evento puede ser uno o más casos, y puede tener varias causas.

NOTA 2: Un evento puede consistir en algo que no sucede.

NOTA 3: Un evento a veces puede ser contemplado como un "incidente" o "accidente".

NOTA 4 Un evento sin consecuencias también puede ser contemplado como una "cerca de la señorita", "incidente", "cerca de Hit" o "cerca de llamada ".

Probabilidad

Posibilidad de que suceda algo

NOTA 1 En la terminología de la gestión de riesgos, la palabra "riesgo" se utiliza para referirse a la posibilidad de que ocurra algo, si se define, mide, o determinar de forma objetiva o subjetiva, cualitativa o cuantitativamente, y se describen utilizando términos generales o las matemáticas (como una probabilidad o frecuencia durante un período de tiempo determinado).

NOTA 2 El término Inglés "riesgo" no tiene un equivalente directo en algunas lenguas, en cambio, el equivalente del término "probabilidad" se utiliza a menudo. Sin embargo, en inglés, "probabilidad" es a menudo de una interpretación restrictiva como un término matemático. Por lo tanto, en la terminología de la gestión de riesgos, "probabilidad" se utiliza con la intención de que deben tener la misma amplia interpretación del término "probabilidad" tiene en muchos idiomas distintos Inglés.

El tratamiento del riesgo

El proceso para modificar el riesgo

NOTA 1: el tratamiento del riesgo puede incluir:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;
- Tomando o aumentar el riesgo con el fin de perseguir una oportunidad;
- La eliminación de la fuente de riesgo;
- Cambiar la probabilidad;
- Cambiando las consecuencias;
- Compartir el riesgo con la otra parte o partes (incluidos los contratos y la financiación de riesgo), y
- Mantener el riesgo de decisiones informada.

NOTA 2 tratamientos de riesgo que lidiar con las consecuencias negativas se refieren a veces como "reducción del riesgo", "riesgo de eliminación "," prevención de riesgos "y" reducción de riesgos".

NOTA 3 tratamiento de los riesgos puede crear nuevos riesgos o modificar los riesgos existentes.

Seguimiento

Control continuo, supervisar, observar críticamente o de determinar el estado a fin de determinar el cambio del nivel de rendimiento requerido o esperado.

NOTA puede ser aplicado a un marco de gestión del riesgo, el proceso de gestión del riesgo, el riesgo de o el control.

Revisar

Actividad emprendida para determinar la conveniencia, la idoneidad y la eficacia de la materia objeto de lograr objetivos establecidos

NOTA revisión puede ser aplicada a un marco de gestión del riesgo, el proceso de gestión del riesgo, el riesgo o el control.

3.6.3. MODELO COSO

El Informe COSO (Committee of Sponsoring Organizations of the Treadway Commission), hace referencia a la importancia de la Tecnología Informática, en relación con el entorno global de control de una organización, pero no proporciona una guía detallada para las empresas que necesitan diseñar e implementar controles específicos para su entorno. En la definición de Control Interno expuesta en el Informe COSO, se indica que los controles internos, independientemente de su adecuado diseño y de la efectividad y eficiencia de su operación, sólo proveen seguridad razonable de que la entidad logre sus objetivos de control. La probabilidad de lograrlos dependerá de las limitaciones que posea el sistema de control

interno, el cual incluye los juicios subjetivos de las personas encargadas de la toma de decisiones, y evidentemente éstos pueden estar sujetos a errores, que podrían generar vulnerabilidades que faciliten la materialización de causas de riesgo.

El marco de control interno sugerido por el documento COSO IC–IF (Marco Integrado de Control Interno), para el cumplimiento de la Ley Sarbanes-Oxley, aborda el tema de los controles de TI, pero no establece requisitos para tales objetivos de control y las actividades de control relacionadas. El control interno (CI) es un proceso, efectuado por la junta de directores de la entidad, la gerencia y cualquier otro personal designado por los anteriores. El CI se diseña para proporcionar una seguridad razonable en cuanto a la consecución de los objetivos relacionados con las operaciones, la elaboración y confiabilidad de los informes y el cumplimiento de leyes y regulaciones (ver figura 3.5).

Figura 3. 5: COSO

Fuente: COSO ERM: Marco de Gestión Integral de Riesgo, 2004

3.6.4. MARCO DE REFERENCIA COBIT 5

Es el conjunto de mejores prácticas para el manejo de información, creado por la Asociación para la Auditoría y Control de Sistemas de Información – ISACA.

COBIT 5, provee un marco de referencia de Gobierno y Gestión de TI en las empresas y herramientas de soporte que permiten a la alta dirección reducir la brecha entre las necesidades de control, los asuntos técnicos y los riesgos del negocio. COBIT permite el

desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones, enfatizando en el cumplimiento normativo, ayudando a las organizaciones a aumentar el valor obtenido de TI, facilitando su alineación y simplificando la implementación del marco de referencia.

El marco de *COBIT 5* se basa en cinco (5) principios claves que incluyen una amplia guía para los facilitadores de gobierno y gestión de TI en la empresa, (ver figura 3.6).

Figura 3. 6: Principios de COBIT 5

Fuente: COBIT 5. Principios

Principio 1

Las entidades existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. Creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. (ver figura 3.7) Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las empresas comerciales o de servicio público para entidades gubernamentales.

Figura 3. 7: Objetivo de Gobierno

Fuente: COBIT 5. El objetivo de gobierno. Creación de valor.

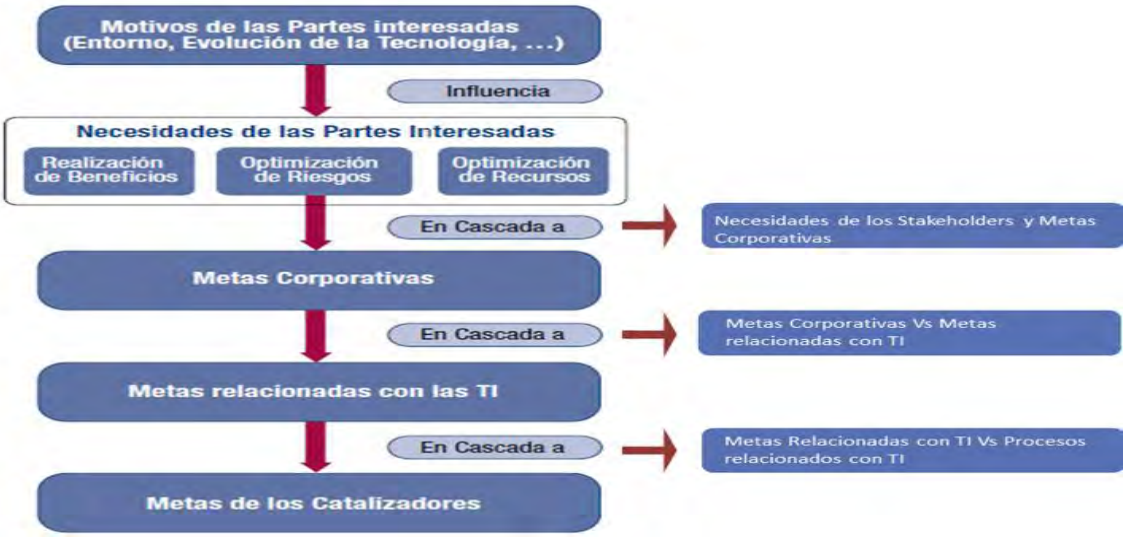
Cascada de Metas de COBIT 5

Cada empresa opera en un contexto diferente; este contexto está determinado por factores externos e internos.

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI.

El marco de referencia de *COBIT 5* establece un análisis en cascada que parte de las necesidades de los interesados y culmina con las metas de los procesos catalizadores, (ver Figura 3.8).

Figura 3. 8: Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa



Fuente: COBIT 5. "Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa"

COBIT 5 define 17 objetivos genéricos, que incluye la siguiente información:

- La dimensión del Cuadro de Mando Integral (CMI) en la que encaja la meta corporativa;
- Las metas corporativas;
- La relación con los tres objetivos principales de gobierno -- realización de beneficios, optimización de riesgos y optimización de recursos ('P' indica una relación primaria y 'S' una relación secundaria, es decir una relación menos fuerte).

Cuadro de Mando Integral

Todas las organizaciones tienen objetivos y planes estratégicos. Si no, nada se sostendría. Los objetivos tienen que estar siempre presentes, saber cuándo se están cumpliendo y cuando

la empresa se está desviando de ellos. Para que esto no quede en simples ideas hay herramientas que ayudan a percibirlo, una de ellas es el CMI.

El CMI (*Balanced Scorecard* – BSC) es una herramienta de administración de empresas que muestra continuamente cuándo una compañía y sus empleados alcanzan los resultados definidos por el plan estratégico. Adicionalmente, un sistema como el CMI permite detectar las desviaciones del plan estratégico y expresar los objetivos e iniciativas necesarios para reconducir la situación.

El CMI NO es un Sistema de Control, como muchas empresas y profesionales afirman, al pensar de este modo le quitamos la esencia misma de esta herramienta, ya que fue diseñada para administrar la estrategia de largo plazo de la empresa y no para controlar determinadas acciones administrativas.

Cascada de Metas de Empresa a Metas Relacionadas con las TI

El logro de metas empresariales requiere un número de resultados relacionados con las TI, que están representados por las metas relacionadas con la TI. Se entiende como relacionados con las TI a la información y tecnologías relacionadas, y las metas relacionadas con las TI se estructuran en dimensiones del CMI. COBIT 5 define 17 metas relacionadas con las TI, indicadas en la figura 3.9

Figura 3. 9: Metas relacionadas con las TI

Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Fuente: COBIT 5. Metas relacionadas con las TI

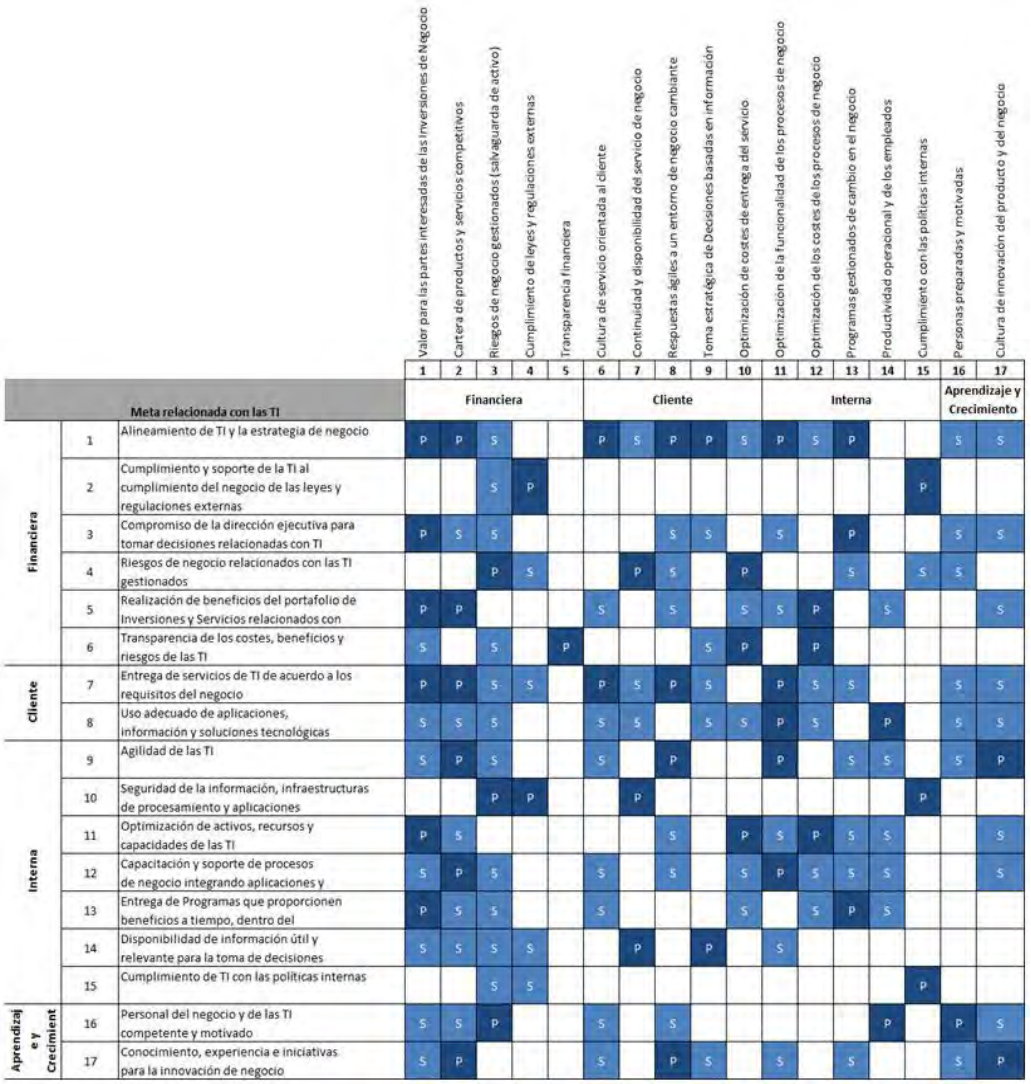
Mapeo detallado de las metas de empresa y las metas relacionadas con las TI

El propósito de la tabla de mapeo de la figura 3.10 es mostrar cómo las metas empresariales son soportadas (o se traducen) en objetivos relacionados con TI. Por este motivo, la tabla contiene la siguiente información:

- Las columnas contienen, agrupados por dimensión del CMI, los 17 objetivos genéricos corporativos de COBIT 5.
- En horizontal, los 17 objetivos relacionados con TI, igualmente agrupados por dimensión del CMI.
- El mapeo de cómo cada objetivo corporativo es soportado por los objetivos TI relacionados. Este mapeo se expresa usando la siguiente escala:

- "P" para principal, cuando hay una importante relación, es decir, las metas relacionadas con TI que son el pilar imprescindible para conseguir los objetivos de la empresa.
- "S" para secundario, cuando todavía hay un vínculo fuerte, pero menos importante, es decir, las metas relacionadas con TI son un soporte secundario para los objetivos de la empresa.

Figura 3. 10: Mapeo metas corporativas y metas TI



		Meta relacionada con las TI	1 Valor para las partes interesadas de las Inversiones de Negocio	2 Cartera de productos y servicios competitivos	3 Riesgos de negocio gestionados (salvaguarda de activo)	4 Cumplimiento de leyes y regulaciones externas	5 Transparencia financiera	6 Cultura de servicio orientada al cliente	7 Continuidad y disponibilidad del servicio de negocio	8 Respuestas ágiles a un entorno de negocio cambiante	9 Toma estratégica de Decisiones basadas en información	10 Optimización de costes de entrega del servicio	11 Optimización de la funcionalidad de los procesos de negocio	12 Optimización de los costes de los procesos de negocio	13 Programas gestionados de cambio en el negocio	14 Productividad operacional y de los empleados	15 Cumplimiento con las políticas internas	16 Personas preparadas y motivadas	17 Cultura de innovación del producto y del negocio
			Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	1	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del	P	S	S			S				S		S	P	S			
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Fuente: COBIT 5. Mapeo metas corporativas y metas TI

Cascada de Metas Relacionadas con las TI Hacia Metas Catalizadoras

Alcanzar metas relacionadas con las TI requiere la aplicación satisfactoria y el uso de varios catalizadores. Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir.

El marco de referencia COBIT 5 describe siete categorías de catalizadores:

1) Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
2) Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
3) Las estructuras organizativas son las entidades de toma de decisiones clave en una organización.
4) La Cultura, ética y comportamiento de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
5) La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
6) Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

7) Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

Principio 2: Cubrir la empresa extremo-a-extremo

COBIT 5 contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo a extremo y para toda la empresa.

COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI, basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo-a-extremo, es decir, incluyendo todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

El enfoque de gobierno extremo-a-extremo que es la base de COBIT 5 está representado en la figura 3.11, mostrando los componentes clave de un sistema de gobierno.

Figura 3. 11: Gobierno

Fuente: COBIT 5. Gobierno

Principio 3: Aplicar un Marco de Referencia Único Integrado

Existen una infinidad de estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

1. Principios, Políticas y Marcos de Trabajo
2. Procesos
3. Estructuras Organizativas
4. Cultura, Ética y Comportamiento
5. Información
6. Servicios, Infraestructuras y Aplicaciones
7. Personas, Habilidades y Competencias

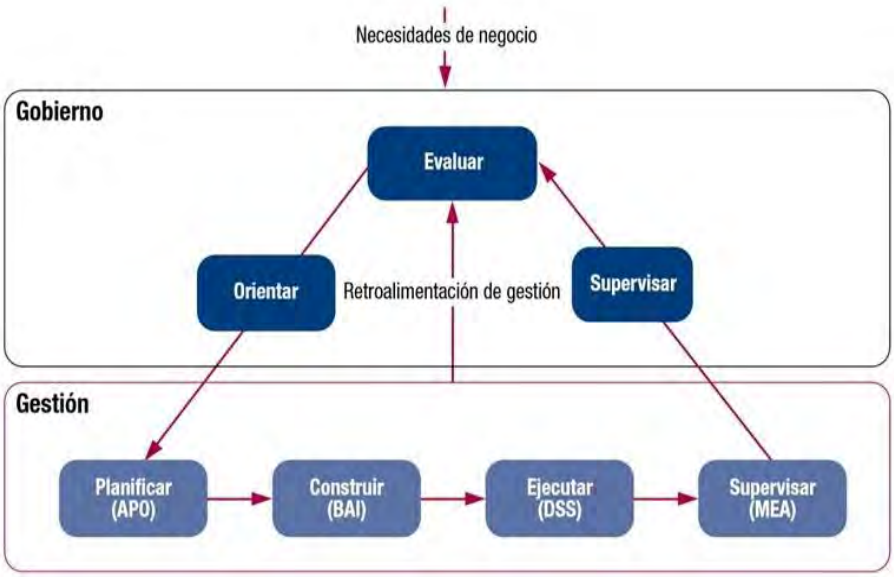
Principio 5: Separar el Gobierno de la Gestión

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

Modelo de Referencia de Procesos de COBIT 5

COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas, tal y como se muestra en la figura 3.10

Figura 3. 12: Gestión y Gobierno



Fuente: COBIT 5. Gobierno y gestión

COBIT 5 tiene definidos 37 procesos agrupados en cinco (5) dominios.

- El marco teórico de Gobierno y Gestión de TI enfocado en los 5 dominios y 37 procesos de COBIT 5:

Evaluar, Orientar y Supervisar

1. EOS01 Asegurar que se fija el Marco de Gobierno y su Mantenimiento
2. EOS02 Asegurar la Entrega de Valor
3. EOS03 Asegurar la Optimización de los Riesgos

4. EOS04 Asegurar la Optimización de los Recursos
5. EOS05 Asegurar la Transparencia a las partes interesadas

Alinear, Planear y Organizar

6. APO01 Administrar el Marco de la Administración de TI
7. APO02 Administrar la Estrategia
8. APO03 Administrar la Arquitectura Corporativa
9. APO04 Administrar la Innovación
10. APO05 Administrar el Portafolio
11. APO06 Administrar el Presupuesto y los Costos
12. APO07 Administrar el Recurso Humano
13. APO08 Administrar las Relaciones
14. APO09 Administrar los Contratos de Servicios
15. APO10 Administrar los Proveedores
16. APO11 Administrar la Calidad
17. APO12 Administrar los Riesgos
18. APO13 Administrar la Seguridad

Monitorear, Evaluar y Valorar

18. MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento
19. MEA02 Monitorear, Evaluar y Valorar el Sistema de Control Interno
20. MEA03 Monitorear, Evaluar y Valorar el Cumplimiento con Requisitos Externos

Construir, Adquirir e Implementar

21. BAI01 Administrar Programas y Proyectos
22. BAI02 Administrar la Definición de Requerimientos

23. BAI03 Administrar la Identificación y Construcción de Soluciones
24. BAI04 Administrar la Disponibilidad y Capacidad
25. BAI05 Administrar la Habilitación del Cambio
26. BAI06 Administrar Cambios
27. BAI07 Administrar la Aceptación de Cambios y Transiciones
28. BAI08 Administrar el Conocimiento
29. BAI09 Administrar los Activos
30. BAI10 Administrar la Configuración

Entregar, Servir y Dar Soporte

31. DSS01 Administrar las Operaciones
32. DSS02 Administrar las Solicitudes de Servicios y los Incidentes
33. DSS03 Administrar Problemas
34. DSS04 Administrar la Continuidad
35. DSS05 Administrar los Servicios de Seguridad
36. DSS06 Administrar los Controles en los Procesos de Negocio

- Procesos Habilitadores COBIT 5;
- Modelo de Evaluación de Procesos COBIT 5;
- Guía de Autoevaluación COBIT 5.

CAPITULO IV

DESARROLLO DEL MÉTODO

CAPÍTULO IV

DESARROLLO DEL MÉTODO

La información es un activo clave para toda entidad o empresa y desde el momento en que la información se crea hasta que es destruida, o sea en cumplimiento a su ciclo de vida, la tecnología juega un papel importante.

La TI tiene un avance vertiginoso y se ha generalizado su uso tanto en entidades públicas y privadas. Las TI como parte inherente del negocio, son consideradas un factor clave en la productividad y competitividad de una organización, de allí que los riesgos derivados de su operación se convierten en aspectos críticos que requieren ser tratados a través de un adecuado gobierno y gestión

Debemos esforzarnos en generar valor al negocio con las inversiones en TI, alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente, mantener los riesgos relacionados con TI en un nivel aceptable, optimizar el coste de los servicios y tecnologías de TI, entre otros.

Un modelo o herramienta, un conjunto de buenas prácticas, ayuda de forma muy significativa a que una organización gobierne y dirija adecuadamente las TI, como parte de su proceso de negocio.

En el gobierno de las TI el hilo conductor y que siempre debe tenerse en cuenta es el riesgo del negocio (qué beneficios a qué nivel aceptable de riesgo y a qué costo). Entendiéndose de esta manera que las necesidades del negocio son prioritarias.

El desarrollo e implantación de un determinado modelo no es una tarea aislada del área de TI, es de responsabilidad de la alta dirección, desde su más alto nivel el que deben involucrarse. Sin este apoyo no se podrán obtener los recursos necesarios.

Cuando se implemente esta propuesta de modelo, deberá ser reconocida por toda la organización, en la medida que afectarán, de una forma u otra, a sus tareas cotidianas, e inclusive a su desarrollo estratégico. Por tanto, la formación antes y después de su implantación es fundamental.

4.1. FUNDAMENTOS DEL MÉTODO

Las organizaciones tienen metas que lograr contempladas en su misión y visión, para llegar al cumplimiento de estas se tienen que enfrentar a un entorno que las obliga a buscar diariamente oportunidades de mejora en la realización de sus procesos, buscando ventajas competitivas en el mercado.

Las entidades enfrentan diversos tipos de riesgos, ya sean riesgos propios del negocio en que se desenvuelven, financieros y operacionales, como riesgos ajenos a su operación, sociales, ambientales, y éticos, los cuales son cada día más globales y complejos producto del entorno dinámico en que se encuentran insertas. Por ello las entidades deben ser hábiles en identificar y gestionar estos riesgos para encausarlos a niveles aceptables, con el fin que sean percibidos como oportunidades y no como amenazas.

El modelo propone un marco de trabajo que ayuda a las entidades públicas y privadas a alcanzar sus objetivos para la gestión de riesgos de TI institucionales. El modelo propuesto es genérico y útil para entidades pequeñas, medianas y grandes. Se pretende estar preparados para asumir riesgos que otros no asumirían. Estas expectativas divergentes y algunas veces en conflicto necesitan ser tratadas con efectividad apoyados en el estándar Cobit 5, que es un marco de gobierno de TI que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio.

4.1.1. CARACTERÍSTICAS DEL MODELO

El modelo que se propone a ser implementada tiene las siguientes características:

Está enfocada a diferentes áreas funcionales, el modelo de gestión de riesgos es aplicable a todo tipo de áreas y/o departamentos de la organización, específicamente en el "INSTITUTO TECNOLOGICO MARCELO QUIROGA SANTA CRUZ"

Es genérica, el modelo será genérico para poder ser aplicado en cada unidad funcional, como también aplicado por la alta gerencia, independiente a la tecnología.

Esta adecuada a la realidad de nuestro país, la brecha cultural entre los países desarrollados y los países subdesarrollados como la nuestra, de alguna manera incidirán en el alcance del modelo que se plantea.

4.1.2. OBJETIVOS GENERALES DEL MODELO

Para aplicar el modelo se requiere la participación efectiva de los interesados de la organización, como los accionistas, unidades de auditoria interna, unidades de sistemas como principales entes primarios. El método trata de satisfacer los siguientes objetivos:

- **Objetivos para la alta gerencia,** los diferentes niveles de autoridad en la organización luego de brindar apoyo técnico y económico para la implantación del modelo podrán contar con información oportuna y fiable para una adecuada toma de decisiones, manteniendo el riesgo relacionado con TI a niveles aceptables.
- **Objetivos para unidades de auditoria interna,** incentivar a que las unidades de auditoria interna, no solo se dediquen al control interno financiero, mas al contrario realicen esfuerzos para que efectúen una adecuada evaluación técnica y administrativa de los recursos tecnológicos, con el fin de minimizar los riesgos.

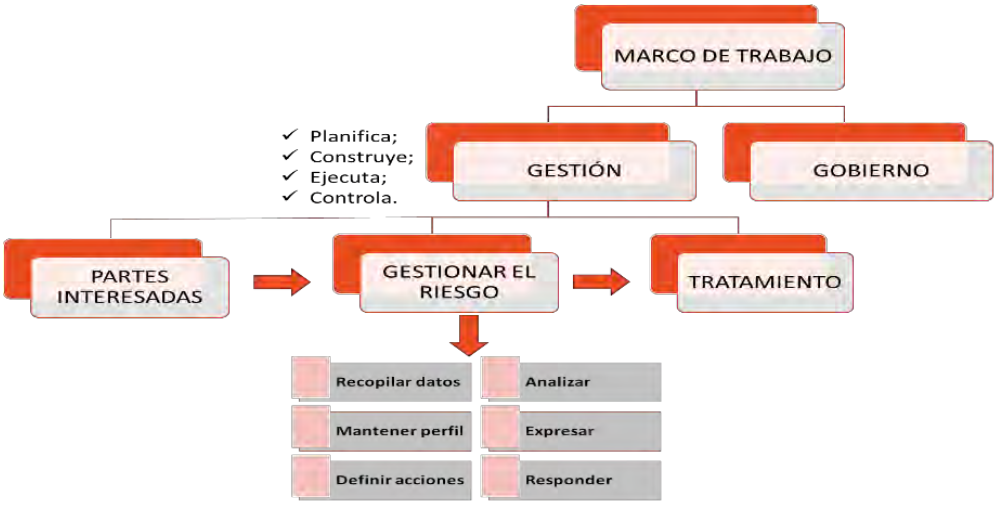
4.2. DESARROLLO DEL MÉTODO

Los riesgos relacionados de TI existen, independientemente de si son descubiertos o reconocidos por una organización. En este contexto es importante identificar y gestionar potencialmente los asuntos importantes de riesgo de TI, a diferencia del resto de riesgos, ya que éste puede no ser rentable.

El éxito de la gestión del riesgo dependerá de la eficacia del modelo de gestión que se propone. El modelo ayuda en la gestión de los riesgos de manera efectiva a través de la aplicación del proceso de gestión del riesgo en los diferentes niveles y dentro de contextos específicos de la organización. El modelo se podrá utilizar como base para la toma de decisiones y la rendición de cuentas en todos los niveles pertinentes de organización.

El modelo o marco de trabajo es un proceso iterativo, basado en el conocimiento, valoración, tratamiento y monitoreo de los riesgos y sus impactos en el negocio, se dividirá en 2 áreas y éstas a su vez en sub áreas, (ver figura 4.1):

Figura 4. 1: Marco de Trabajo



Fuente: Elaboración propia

4.2.1. GOBIERNO

El gobierno de riesgos de TI, es el sistema por el cual se dirigen y controlan las incertidumbres presentes y futuras que generan las tecnologías de información en la organización (ISO/IEC 38500:2008).

Las TI como parte inherente del negocio, son un factor clave en la productividad y competitividad de una organización, de allí que los riesgos derivados de su operación se convierten en aspectos críticos que requieren ser tratados a través de un adecuado gobierno y gestión.

El término "gobierno", hoy en día, ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos hechos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

La unidad de riesgos y la alta gerencia de la entidad deben aceptar a las TI como cualquier otra parte importante de hacer negocios, deben trabajar en forma colaborativa y constructiva, de modo que se incluya la TI en el enfoque del gobierno.

Debemos gobernar bajo una mirada holística, abarcando al negocio por completo, es decir, de principio a fin (de extremo-a-extremo), considerando intereses relacionados con TI de las partes interesadas internas y externas.

Las empresas existen para crear valor para sus partes interesadas. En consecuencia, cualquier entidad pública o privada tendrá la creación de valor como objetivo de gobierno. La creación de valor significa obtener beneficios a un coste óptimo de recursos mientras se optimiza el riesgo. Ver figura 4.2

Figura 4. 2: Creación de Valor

Fuente: Elaboración propia

Luego, debemos aplicar el Principio 5 de Cobit 5: Separar el Gobierno de la Gestión. Para asegurar que se evalúan las necesidades, condiciones y opciones de las partes interesadas. Determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

Las necesidades de las partes interesadas se transforman en estrategia corporativa practicable. La figura 4.2 debe dar lugar a la cascada de metas:

- Objetivos de la entidad;
- Objetivos de las Tecnología de la Información;
- Objetivos de los Catalizadores.

El logro de las metas corporativas requiere una serie de resultados TI, representados por las metas relacionadas con TI que se encuentran estructuradas en las dimensiones del Cuadro de Mando Integral TI.

COBIT 5 define 17 metas TI. En la práctica de mapeo con los objetivos de Tecnología de la Información y tecnología relacionada, el listado de la figura 4.3.

Figura 4. 3: Metas de TI

Dimension del CMI	Objetivo de la Empresa	Relacion con los Objetivos de Gobierno		
		Realizacion de Beneficios	Optimizacion de riesgos	Optimizacion de Recursos
Financiera	1. Valor para Partes Interesadas	P		S
	2.Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera y riesgos de TI	P	S	S
Usuario	6. Cultura de servicio orientada al usuario	P		S
	7. Continuidad y disponibilidad del servicio		P	
	8.Uso adecuado de aplicaciones, información y soluciones tecnológicas	P		S
	9. toma estrategias de Decision basada en informacion	P	P	P
	10. Optimizacion de coste de entrega del servicio	P		P
Interna	11. Agilidad de las TI	S	P	P
	12. Optimizacion de los costes de los procesos de negocio			P
	13. Programas gestionados de cambio en el empleados	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las politicas internas		P	
Aprendizaje y Crecimiento	16. personas preparadas y motivadas	S	P	P
	17. cultura de innovacion de producto y negocio	P		

Fuente: Elaboración propia (P=primario, S=segundario)

Desde la perspectiva de gobierno de TI, aplicando COBIT 5.0 se obtiene tabla 4.1.

Tabla 4. 1: Gobierno

DOMINIO	PROCESO	ÁREAS CLAVE
Evaluar, Dirigir y Supervisar (EDM por sus siglas en inglés Evaluate, Direct and Monitor)	EDM03 Asegurar la optimización del riesgo.	EDM03.01 Evaluar la gestión de riesgos. EDM03.02 Orientar la gestión de riesgos. EDM03.03 Supervisar la gestión de riesgos.

Fuente: elaboración propia, basado en el dominio de Cobit 5

4.2.2. GESTIÓN

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En muchas entidades, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Se debe aplicar los siguientes principios:

- ✓ **Satisfacer las Necesidades de las Partes Interesadas:** Las entidades existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.
- ✓ **Cubrir la Empresa Extremo-a-Extremo:** Cubrir todas las funciones y procesos dentro de la empresa; no enfocarse sólo en la "función de TI", sino tratar la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa. Incluir tanto a interesados internos como externos;
- ✓ **Aplicar un Marco de Referencia Único Integrado:** Existen varios estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para la gestión de las Ti de la entidad.
- ✓ **Hacer Posible un Enfoque Holístico:** La gestión de las TI de la empresa requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos basados en catalizadores (enablers) que en general se definen como cualquier cosa que puede ayudar a conseguir las metas de la empresa.
- ✓ **Separar el Gobierno de la Gestión**.

Desde la perspectiva de gestión de TI, aplicando COBIT 5.0 se obtiene la tabla 4.2.

Tabla 4. 2: Gestión

DOMINIO	PROCESO	ÁREAS CLAVE
Alinear, Planificar y Organizar (APO)	APO12 Gestionar el riesgo. (permite identificar, evaluar y reducir los riesgos de TI de forma continua)	**APO12.01 Recopilar datos.** Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI. **APO12.02 Analizar el riesgo.** Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo. **APO12.03 Mantener un perfil de riesgo.** Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados. **APO12.04 Expresar el riesgo.** Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada. **APO12.05 Definir un portafolio**

		de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio. **APO12.06 Responder al riesgo.** Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI

Fuente: Elaboración propia, basado en el dominio de Cobit 5

4.2.1.1.GESTIONAR EL RIESGO

Este proceso se encarga de identificar, evaluar y reducir los riesgos de TI de forma continua.

Para implementar el modelo, se considera las áreas clave del "INSTITUTO TECNOLOGICO MARCELO QUIROGA SANTA CRUZ" que están relacionados con las tecnologías de información y su Plan Estratégico, a efectos de establecer y fortalecer los controles necesarios en aquellos que así lo requieran. En la identificación de riesgos se consideran los efectos que una mala gestión pueda tener en la imagen del "INSTITUTO TECNOLOGICO MARCELO QUIROGA SANTA CRUZ", las pérdidas producto de inversiones que no generen réditos, y las orientaciones estratégicas.

Estrategia

La estrategia para la gestión de riesgos se basa en los siguientes aspectos:

- Utilizar los sub procesos de COBIT por guía y referencia para la identificación de riesgos de gestión.
- Complementar la identificación de riesgos basándose en los procesos del instituto, esto para identificar riesgos operativos.

- Utilizar escalas de calificación de los riesgos (impacto, probabilidad, exposición) de acuerdo con modelos generalmente aceptados.

4.2.1.1.1. RECOPILAR DATOS

Identificar y recopilar datos relevantes para catalizar una identificación, ver Tabla 4.3, análisis y notificación efectiva de riesgos relacionados con TI.

Los riesgos identificados están clasificados por categorías: Infraestructura, operación, gestión, seguridad y recursos humanos.

Tabla 4. 3: Identificar y Recopilar Datos

NRO.	DETALLE DEL RIESGO	CATEGORIA
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Gestión
2	Desarrollar productos que no cumplen con las especificaciones.	Gestión
3	Desarrollar productos basados en requerimientos incorrectos.	Gestión
4	Versiones de software desactualizadas	Gestión
5	Adquirir software sin programas fuentes	Gestión
6	Equipo dañado no puede ser reparado	Operación
7	Red inalámbrica insegura	Operación
8	Obsolescencia de la infraestructura tecnológica	Gestión
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Gestión
10	No existe guía de usuario para el uso del sistema	Gestión
11	Se adquiere equipo no compatible con la infraestructura en uso	Gestión
12	Trabajar directamente en equipos de producción	Operación
13	Versiones de software para desarrollo y producción diferentes.	Operación
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Operación
15	Instalación de parches sin seguir las recomendaciones del proveedor	Operación
16	No existe contrato de mantenimiento	Gestión
17	Tiempo de respuesta degradado	Operación
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	Gestión
19	Suspensión de servicio de Internet	Infraestructura
20	Fallas en los equipos de comunicaciones	Infraestructura
21	Equipo de usuario final inseguro	Seguridad
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	Seguridad
23	No se conocen los costos asignados a los servicios prestados por TI	Gestión

24	Personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación	Gestión
25	Personal no cuenta con las actitudes y aptitudes para hacer uso de la información	RRHH
26	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI	Operación
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	Operación
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	Operación
29	Alteración o pérdida de la información registrada en base de datos o equipos.	Seguridad
30	Información desactualizada o incorrecta	Operación
31	Acceso no autorizado a la información	Seguridad
32	No aplicación de las políticas para la generación de respaldos	Operación
33	Suspensión de servicios sin seguir el procedimiento establecido	Operación
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	Gestión
35	No contar con la documentación de los procesos de TI	Gestión
36	Uso de software no licenciado	Seguridad
37	Se tiene Plan Estratégico desactualizado	Gestión
38	Adquisición de tecnologías que no aportan valor a la organización	Gestión
39	No se tienen documentados los canales de comunicación	Gestión
40	No se tiene dominio sobre las herramientas en uso	RRHH
41	Equipo de trabajo con baja motivación y no comprometido con el logro de los objetivos	RRHH
42	Desarrollar productos que no cumplen con los requerimientos de calidad	Operación
43	No administrar los riesgos de TI	Gestión
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	Gestión

Fuente: Elaboración propia

4.2.1.1.2. ANALIZAR EL RIESGO

Criterios de evaluación de riesgos

Para la evaluación de riesgos se utilizarán, como valores primarios, la calificación de impacto y probabilidad de cada riesgo. Para ambos casos se utilizarán tablas de 5 valores con las equivalencias que se visualizan en la tabla 4.4 incisos a) y b).

Tabla 4. 4: Criterios de Evaluación de Riesgos

PROBABILIDAD	
P	SIGNIFICADO
1	Casi nunca
2	Poco probable
3	Probable
4	Muy probable
5	Casi seguro

a)

IMPACTO	
I	SIGNIFICADO
1	Menor
2	Regular
3	Significativo
4	Importante
5	Alto impacto

b)

Fuente: Elaboración propia

En base a los valores se calculará el nivel de exposición y la severidad de los riesgos representándolos en el mapa térmico.

Para clasificar los riesgos se utilizarán 5 categorías asociadas con el origen del riesgo. Se utilizarán criterios de referencia específicos para cada categoría con el propósito de facilitar la evaluación de impacto para cada riesgo.

Para calificar la severidad se utilizará una tabla de referencia con 4 valores que se determina según la calificación del impacto y la probabilidad, es decir el nivel de exposición y para el mapa térmico se presenta el modelo, ver Tabla 4.5, incisos c) y d).

Tabla 4. 5: Nivel de Exposición y la Severidad de los Riesgos

IMPACTO	
I	SIGNIFICADO
1	Baja
2	Moderada
3	Alta
4	Extrema

c)

IMPACTO					
5	M	A	E	E	E
4	M	A	A	E	E
3	B	M	A	A	E
2	B	M	M	A	A
1	B	B	B	M	M
	1	2	3	4	5

PROBABILIDAD

d)

Fuente: Elaboración propia

Categorías de los riesgos

La tabla 4.6, muestra las categorías utilizadas:

Tabla 4. 6: Categorías de los Riesgos

CATEGORIA	DETALLE
GESTIÓN	Riesgos relacionados con la ausencia o aplicación incorrecta de métodos de gestión de TI.
OPERACIÓN	Incumplimiento de directrices, procedimientos y metodologías y estándares en los procesos operativos.
INFRAESTRUCTURA	Riesgos relacionados con las fallas potenciales de la infraestructura tecnológica utilizada en el instituto.
SEGURIDAD	Eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información.
RECURSO HUMANO	Relacionados con el desempeño y regularidad de los recursos humanos.

Fuente: Elaboración propia

Impacto de los riesgos según su categoría. Ver Tabla 4.7

Tabla 4. 7: Impacto de los Riesgos según su Categoría

GESTIÓN		
I	**SIGNIFICADO**	**CRITERIO DE CALIFICACIÓN**
5	Mayor	Evento que impedirá el logro de las metas institucionales
4	Importante	El logro de metas se ve afectado de manera importante.
3	Significativo	Evento que representará un retraso significativo en el logro de metas institucionales
2	Regular	El evento afecta levemente el logro de metas de la entidad
1	Menor	Evento que afecta la gestión de la entidad sin llegar a impactar en el logro de las metas
OPERACIÓN		
I	**SIGNIFICADO**	**CRITERIO DE CALIFICACIÓN**
5	Mayor	Evento que paraliza la prestación de servicios por parte de la unidad afectando a la entidad de manera considerable
4	Importante	Evento que provoca la interrupción parcial de servicios
3	Significativo	Evento que provoca interrupciones intermitentes
2	Regular	Evento que provoca la interrupción momentánea de los servicios, esta interrupción es percibida por la institución. Evento que provoca una disminución en tiempos de respuesta que experimentan los usuarios.
1	Menor	Evento que afecta sólo las operaciones de la entidad
INFRAESTRUCTURA		
I	**SIGNIFICADO**	**CRITERIO DE CALIFICACIÓN**
5	Mayor	Falla severa de un componente de infraestructura tecnológica que impide la operación normal de la entidad

4	Importante	Falla en un componente que afecta parcialmente la prestación de servicios
3	Significativo	Falla en un componente que afecta de manera intermitente la prestación de servicios
2	Regular	Falla en un equipo que afecta la prestación de servicios sólo en la unidad de sistemas
1	Menor	Falla en un componente que puede ser sustituido de inmediato por mantener equipo similar en inventario. Se afecta la operación de la institución por minutos.
SEGURIDAD		
I	**SIGNIFICADO**	**CRITERIO DE CALIFICACIÓN**
5	Mayor	La seguridad es vulnerada y se desconocen sus efectos. Un ente no autorizado tiene acceso a información confidencial. Los datos de la entidad han sido alterados
4	Importante	Un ente no autorizado tiene acceso a información sensitiva.
3	Significativo	Se reciben ataques masivos sobre la plataforma. Un funcionario de la institución tiene acceso a información a la cual no está autorizado
2	Regular	Entes no autorizados tienen acceso a información parcial en modo consulta. Interrupción de 4 horas en la disponibilidad de la información
1	Menor	Hay intentos de acceso a la información. Interrupción momentánea en la disponibilidad de la información
RECURSOS HUMANOS		
I	**SIGNIFICADO**	**CRITERIO DE CALIFICACIÓN**
5	Mayor	Se prescinde de un funcionario importante para el logro de las metas

4	Importante	Los objetivos a lograr exceden las cargas de trabajo de los recursos asignados a la unidad
3	Significativo	No se tiene participación del patrocinador para el logro de los objetivos
2	Regular	Evento que provoca que un funcionario exceda en un 10% el tiempo estimado para finalizar una actividad
1	Menor	Se asignan objetivos adicionales que afectan levemente la carga de trabajo

Fuente: Elaboración propia

Identificación de causas

Cada uno de los riesgos identificados está asociado con una o varias causas, conocer las causas es importante para enfocar los posteriores esfuerzos de mitigación y contingencia, así como para calificar los controles existentes. Podemos ver la Tabla 4.8:

Tabla 4. 8: Identificación de Causas

NRO.	DETALLE DEL RIESGO	CAUSAS
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	No se validó el cumplimiento de la solución automatizada.
2	Desarrollar productos que no cumplen con las especificaciones.	No se validaron los componentes del producto
3	Desarrollar productos basados en requerimientos incorrectos.	No existe contrato de mantenimiento.
4	Versiones de software desactualizadas	No existe contrato de mantenimiento.
5	Adquirir software sin programas fuentes	Ausencia de validación de requerimientos.
6	Equipo dañado no puede ser reparado	No hay contrato de mantenimiento.
7	Red inalámbrica insegura	La red es vulnerable por configuración inadecuada
8	Obsolescencia de la infraestructura tecnológica	No se tiene la experiencia para actualizarla.
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Proceso de desarrollo de deficiente
10	No existe manual técnico	Se omitió el manual de usuario

11	Se adquiere equipo no compatible con la infraestructura en uso	Elaboración de especificaciones incorrectas.
12	Trabajar directamente en equipos de producción	Se obtuvieron passwords del ambiente de producción.
13	Versiones de software para desarrollo y producción diferentes.	No se han actualizado
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Fallas de hardware y software superan el estimado realizado.
15	Instalación de parches sin seguir las recomendaciones del proveedor	No se tiene registro de modificaciones
16	No existe contrato de mantenimiento	No se cuenta con el presupuesto.
17	Tiempo de respuesta degradado	Servidores ocasionalmente degradados y saturados
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	No se planificaron las compras con base al crecimiento
19	Suspensión de servicio de Internet	Fallas en el equipo del proveedor del servicio
20	Fallas en los equipos de comunicaciones	Inexperiencia del personal
21	Equipo de usuario final inseguro	La instalación de componentes no es controlada
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	Se desconoce la cobertura autorizada para cada privilegio
23	No se conocen los costos asignados a los servicios prestados por TI	No se tiene un modelo de costos
24	Personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación	No se tiene un plan de capacitación autorizado
25	Personal no cuenta con las actitudes y aptitudes para hacer uso de la información	No se tiene cultura de procesos automatizados
26	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI	Personal no capacitado
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	No se tiene un sistema para control de cambios
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	No se tiene el ambiente completo para pruebas preliminares
29	Alteración o pérdida de la información registrada en base de datos o equipos.	Violación de la seguridad
30	Información desactualizada o incorrecta	Registro de datos incorrecta
31	Acceso no autorizado a la información	Violación de la seguridad
32	No aplicación de las políticas para la generación de respaldos	No se cuenta con procedimientos aprobados
33	Suspensión de servicios sin seguir el procedimiento establecido	No se cuenta con plan de contingencias
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	No existe sistema para evaluación del desempeño
35	No contar con la documentación de los procesos de TI	No se tiene manual para Gobierno Corporativo
36	Uso de software sin licencia	No se considera la migración al software libre
37	Se tiene Plan Estratégico desactualizado	No se cuenta con un administrador
38	Adquisición de tecnologías que no aportan valor a la organización	Se instalan tecnologías con base a convenios

39	No se tienen documentados los canales de comunicación	Funcionan muy bien los canales informales
40	No se tiene dominio sobre las herramientas en uso	La transferencia tecnológica no funciona
41	Equipo de trabajo con baja motivación y no comprometido con el logro de los objetivos	Clima laboral no adecuado
42	Desarrollar productos que no cumplen con los requerimientos de calidad	Ausencia de validación de requerimientos
43	No administrar los riesgos de TI	No existe la administración basada en riesgos
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	No se ha brindado la capacitación necesaria.

Fuente: Elaboración propia

4.2.1.1.3. MANTENER UN PERFIL DE RIESGO

.

Mantener inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas).

La primera evaluación corresponde a los riesgos absolutos, es decir, valorar el nivel de severidad de cada riesgo sin tomar en cuenta el efecto de los controles que se aplican actualmente.

Como fue definido anteriormente, la calificación se realiza utilizando dos criterios primarios que son la probabilidad (P) y el impacto (I) de cada riesgo, de esto valores se deriva el nivel de exposición (P * I) y la severidad de los riesgos (se utiliza la escala de colores del mapa térmico para su representación), ver Tabla 4.9:

Tabla 4. 9: Escala de colores del Mapa Térmico

NRO.	RIESGO	P	I	S
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	**3**	**3**	**9**
2	Desarrollar productos que no cumplen con las especificaciones.	**2**	**4**	**8**
3	Desarrollar productos basados en requerimientos incorrectos.	**2**	**4**	**8**
4	Versiones de software desactualizadas	**3**	**4**	**12**
5	Adquirir software sin programas fuentes	**1**	**4**	**4**
6	Equipo dañado no puede ser reparado	**3**	**3**	**9**
7	Red inalámbrica insegura	**5**	**5**	**25**

8	Obsolescencia de la infraestructura tecnológica	**3**	**4**	**12**
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	**3**	**3**	**9**
10	No existe manual de usuario para el uso del sistema	**3**	**3**	**9**
11	Se adquiere equipo no compatible con la infraestructura en uso	**2**	**3**	**6**
12	Trabajar directamente en equipos de producción	**3**	**4**	**12**
13	Versiones de software para desarrollo y producción diferentes.	**4**	**4**	**16**
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	**3**	**4**	**12**
15	Instalación de parches sin seguir las recomendaciones del proveedor	**3**	**3**	**9**
16	No existe contrato de mantenimiento	**3**	**4**	**12**
17	Tiempo de respuesta degradado	**3**	**3**	**9**
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	**3**	**4**	**12**
19	Suspensión de servicio de Internet	**3**	**4**	**12**
20	Fallas en los equipos de comunicaciones	**2**	**5**	**10**
21	Equipo de usuario final inseguro	**4**	**3**	**12**
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	**3**	**4**	**12**
23	No se conocen los costos asignados a los servicios prestados por TI	**3**	**3**	**9**
24	Personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación	**2**	**3**	**6**
25	Personal no cuenta con las actitudes y aptitudes para hacer uso de la información	**2**	**3**	**6**
26	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI	**3**	**3**	**9**
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	**3**	**4**	**12**
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	**3**	**4**	**12**
29	Alteración o pérdida de la información registrada en base de datos o equipos.	**2**	**4**	**8**
30	Información desactualizada o incorrecta	**3**	**4**	**12**
31	Acceso no autorizado a la información	**3**	**5**	**15**
32	No aplicación de las políticas para la generación de respaldos	**3**	**4**	**12**
33	Suspensión de servicios sin seguir el procedimiento establecido	**3**	**3**	**9**
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	**3**	**4**	**12**
35	No contar con la documentación de los procesos de TI	**2**	**3**	**6**
36	Uso de software sin licencia	**3**	**4**	**12**
37	Se tiene Plan Estratégico desactualizado	**4**	**4**	**16**
38	Adquisición de tecnologías que no aportan valor a la organización	**2**	**3**	**6**
39	No se tienen documentados los canales de comunicación	**2**	**3**	**6**
40	No se tiene dominio sobre las herramientas en uso	**3**	**4**	**12**
41	Equipo de trabajo con baja motivación y no comprometido con el logro de los objetivos	**3**	**4**	**12**

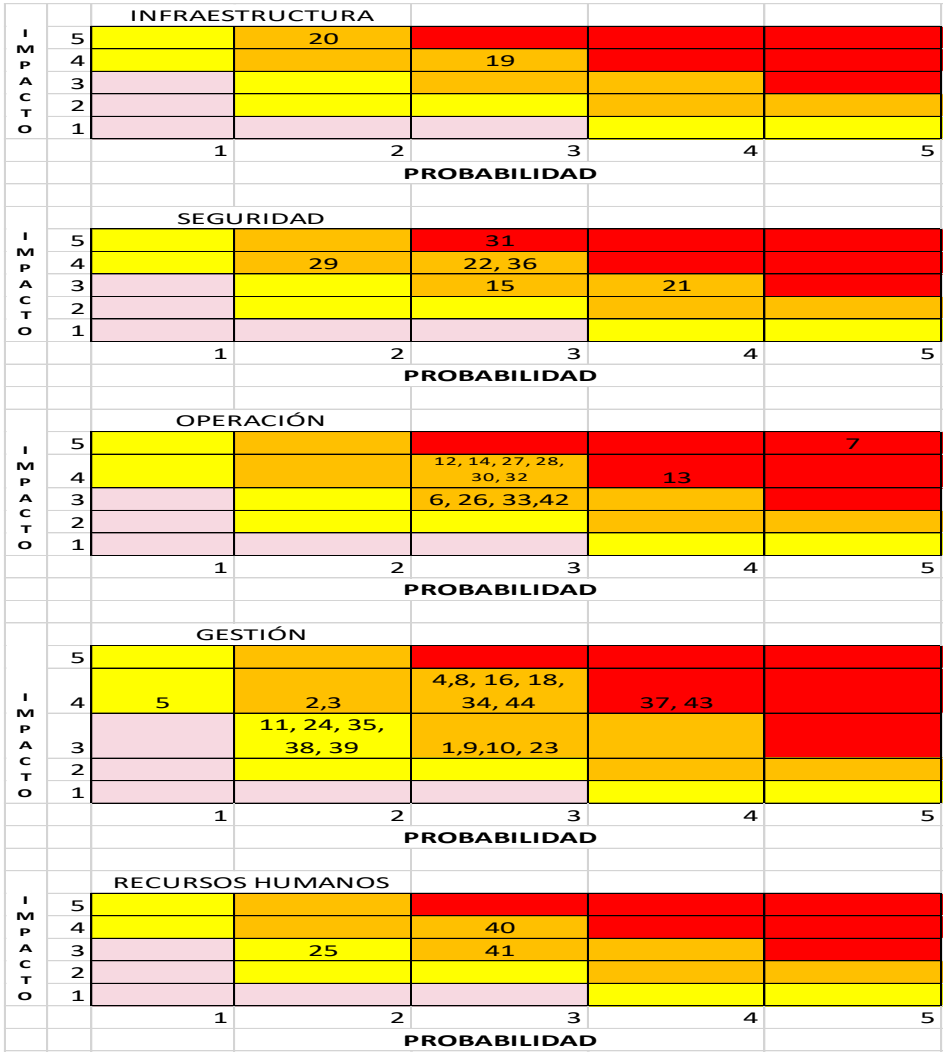
42	Desarrollar productos que no cumplen con los requerimientos de calidad	**3**	**3**	**9**
43	No administrar los riesgos de TI	**4**	**4**	**16**
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	**3**	**4**	**12**

Colores: Verde=Baja, Amarillo=Moderado, Anaranjado=Alta, Rojo=Extremo

Fuente: Elaboración propia

Mapas térmicos riesgos absolutos (ver Tabla 4.10)

Tabla 4. 10: Mapas Térmico Riesgos absolutos



Fuente: Elaboración propia

Identificación de controles (ver Tabla 4.11)

Tabla 4. 11: Identificación de Controles

NRO.	DETALLE DEL RIESGO	CONTROLES
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Se realiza un diagnóstico sobre las necesidades y factibilidad
2	Desarrollar productos que no cumplen con las especificaciones.	Pruebas basadas en casos de uso. Aprobación de fases de análisis y diseño para comprobar el alcance.
3	Desarrollar productos basados en requerimientos incorrectos.	Utilizar casos de uso para especificar los requerimientos. Validación y aprobación de los requerimientos por el patrocinador
4	Versiones de software desactualizadas	Por medio de los contratos de mantenimiento se planifican y aplican actualizaciones del software.
5	Adquirir software sin programas fuentes	Como parte deL plan de licitación se solicitan todos los programas fuente.
6	Equipo dañado no puede ser reparado	Mantener vigentes los contratos de mantenimiento para los equipos. Contar con equipos de respaldos.
7	Red inalámbrica insegura	Se utiliza un plan de seguridad para restringir el acceso a la red inalámbrica.
8	Obsolescencia de la infraestructura tecnológica	Plan de renovación y fortalecimiento de la infraestructura tecnológica. Planificación de adquisiciones con anticipación.
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Supervisión de productos desarrollados. Revisiones formales de los productos por parte de los clientes
10	No existe manual técnico	Se incluye información en línea para cada módulo del sistema de modo que el usuario no necesite el manual. Se desarrollan tutores virtuales sobre la utilización de los sistemas
11	Se adquiere equipo no compatible con la infraestructura en uso	Revisión en el proceso de adquisición de tecnología
12	Trabajar directamente en equipos de producción	Se cuenta con un servidor de aplicaciones.
13	Versiones de software para desarrollo y producción diferentes.	Aplicación del procedimiento para la puesta en producción de los programas nuevos y modificados
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Se han definido responsabilidades y funciones para gestión de cambios
15	Instalación de parches sin seguir las recomendaciones del proveedor	Se revisan las indicaciones de los proveedores. Los parches se aplican primero en equipo de prueba
16	No existe contrato de mantenimiento	Desarrollo periódico de Capacitación.
17	Tiempo de respuesta degradado	Monitoreo de los servicios para determinar cargas de trabajo
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	Se planifica la adquisición de tecnología para mantener la capacidad de procesamiento de información
19	Suspensión de servicio de Internet	Se cuenta con una red que da estabilidad en la operación intern
20	Fallas en los equipos de comunicaciones	Contratos de mantenimiento. Equipo de contingencia y aplicación de respaldos de acuerdo con las políticas definidas
21	Equipo de usuario final inseguro	Aplicación automática de políticas de seguridad por medio de Active Directory. Perfiles de usuarios limitados para instalar software y hacer modificaciones en el equipo
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	El personal que tiene a cargo la implementación de la seguridad
23	No se conocen los costos asignados a los servicios prestados por TI	Se debe mejorar el registro de costos asociados a cada servicio
24	Personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación	Segregación de funciones en forma eficiente
		Periódicamente, por medio del Centro de Capacitación, se

25	Personal no cuenta con las actitudes y aptitudes para hacer uso de la información	Periódicamente, por medio del Centro de Capacitación, se realizan charlas para fomentar la cultura informática
26	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI	Utilización de un software para automatizar la presentación de los incidentes, asignación y seguimiento correspondiente
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	Se implementó una bitácora
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	Se tiene documentada la relación de componentes de TI necesarios para la implementación y funcionamiento de los servicios clave.
29	Alteración o pérdida de la información registrada en base de datos o equipos.	Periódicamente se revisan las copias de respaldos.
30	Información desactualizada o incorrecta	Se revisa la calidad del código generado
31	Acceso no autorizado a la información	Se han definido políticas de TI con responsabilidad para usuario
32	No aplicación de las políticas para la generación de respaldos	Definición de procedimiento de planes de contingencia
33	Suspensión de servicios sin seguir el procedimiento establecido	Bitácoras de cambios en la configuración y suspensión de servic
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	Está pendiente la definición y oficialización del procedimiento para realizar esta actividad
35	No contar con la documentación de los procesos de TI	Se cuenta con descripción de procesos y procedimientos. Los procesos se describen en el plan de TI.
36	Uso de software sin licencia	Los perfiles de usuario tienen restricción para la instalación de software
37	Se tiene Plan Estratégico desactualizado	El Plan Estratégico se revisa anualmente y se ajusta cuando se realizan cambios en la planificación estratégica
38	Adquisición de tecnologías que no aportan valor a la organización	Se revisan las características de acuerdo a necesidades
39	No se tienen documentados los canales de comunicación	Está pendiente de documentarse los canales formales
40	No se tiene dominio sobre las herramientas en uso	Ejecución del programa de capacitación
41	Equipo de trabajo con baja motivación y no comprometido con el logro de los objetivos	Se realizan evaluaciones de clima laboral por año
42	Desarrollar productos que no cumplen con los requerimientos de calidad	Aplicación de estándares y procedimientos de calidad. Capacitación del personal en técnicas de calidad.
43	No administrar los riesgos de TI	Se cuenta con un plan contra contingencias. Anualmente se realiza un ejercicio de valoración de riesgos
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	Se utilizan las instrucciones definidas dentro del marco de gestión de riesgos.

Fuente: Elaboración propia

Evaluación de riesgos controlados (ver Tabla 4.12)

Tabla 4. 12: Evaluación de Riesgos Controlados

NRO.	RIESGO	P	I	S
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	3	4	12
2	Desarrollar productos que no cumplen con las especificaciones.	3	3	9
3	Desarrollar productos basados en requerimientos incorrectos.	2	4	8
4	Versiones de software desactualizadas	3	4	12
5	Adquirir software sin programas fuentes	3	3	9
6	Equipo dañado no puede ser reparado	2	4	8
7	Red inalámbrica insegura	4	4	16
8	Obsolescencia de la infraestructura tecnológica	3	3	9
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	3	3	9
10	No existe manual de usuario para el uso del sistema	3	4	12
11	Se adquiere equipo no compatible con la infraestructura en uso	2	4	8
12	Trabajar directamente en equipos de producción	1	4	4
13	Versiones de software para desarrollo y producción diferentes.	2	4	8
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	2	4	8
15	Instalación de parches sin seguir las recomendaciones del proveedor	3	4	12
16	No existe contrato de mantenimiento	3	4	12
17	Tiempo de respuesta degradado	1	3	3
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	3	4	12
19	Suspensión de servicio de Internet	2	4	8
20	Fallas en los equipos de comunicaciones	2	3	6
21	Equipo de usuario final inseguro	3	4	12
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	2	4	8
23	No se conocen los costos asignados a los servicios prestados por TI	3	3	9
24	Personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación	2	3	6
25	Personal no cuenta con las actitudes y aptitudes para hacer uso de la información	1	3	3
26	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI	1	3	3
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	2	4	8
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	3	4	12
29	Alteración o pérdida de la información registrada en base de datos o equipos.	3	4	12
30	Información desactualizada o incorrecta	2	4	8
31	Acceso no autorizado a la información	3	5	15
32	No aplicación de las políticas para la generación de respaldos	3	4	12
33	Suspensión de servicios sin seguir el procedimiento establecido	2	3	6
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	3	3	9
35	No contar con la documentación de los procesos de TI	3	4	12
36	Uso de software sin licencia	4	4	16
37	Se tiene Plan Estratégico desactualizado	3	4	12
38	Adquisición de tecnologías que no aportan valor a la organización	1	3	3
39	No se tienen documentados los canales de comunicación	2	2	4
40	No se tiene dominio sobre las herramientas en uso	3	4	12
41	Equipo de trabajo con baja motivación y no comprometido con el logro de los objetivos	1	4	4
42	Desarrollar productos que no cumplen con los requerimientos de calidad	3	5	15
43	No administrar los riesgos de TI	4	5	20
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	4	5	20
	Colores: Verde=Baja, Amarillo=Moderado, Anaranjado=Alta, Rojo=Extremo			

Fuente: Elaboración propia

Mapas térmicos riesgos controlados (ver Tabla 4.13)

Tabla 4. 13: Mapas Térmicos Riesgos Controlados

INFRAESTRUCTURA

IMPACTO						
	5					
	4		19			
	3		20			
	2					
	1					
		1	2	3	4	5
		PROBABILIDAD				

SEGURIDAD

IMPACTO						
	5			31		
	4		22	29, 15, 21	36	
	3					
	2					
	1					
		1	2	3	4	5
		PROBABILIDAD				

OPERACIÓN

IMPACTO						
	5			42	7	
	4	12	14, 27, 30, 6 13	28, 32		
	3	26	33			
	2					
	1					
		1	2	3	4	5
		PROBABILIDAD				

GESTIÓN

IMPACTO						
	5				44, 43	
	4		3, 11	35, 4, 16, 1 10, 37		
	3	38	24	5, 2, 8, 18 34, 9, 23		
	2		39			
	1					
		1	2	3	4	5
		PROBABILIDAD				

RECURSOS HUMANOS

IMPACTO						
	5					
	4	41		40		
	3	25				
	2					
	1					
		1	2	3	4	5
		PROBABILIDAD				

Fuente: Elaboración propia

4.2.1.1.4. EXPRESAR EL RIESGO

En esta actividad proporcionamos información sobre el estado actual de exposiciones y oportunidades relacionadas con TI a todas las partes interesadas.

Para facilitar el análisis del nivel de riesgo de los procesos de TI se presenta en la Tabla 4.14 los valores totales de cantidad de riesgos, por cada proceso, en las evaluaciones de riesgos absolutos y riesgos controlados. Posteriormente esta información se presenta en gráficos y cuadros de porcentajes:

Tabla 4. 14: Valores Totales de Cantidad de Riesgos

PROCESOS DE TI	SEVERIDAD	RIESGOS ABSOLUTOS	RIESGOS CONTROLADOS
Infraestructura	Extrema	0	0
	Alta	2	1
	Moderada	0	1
	Baja	0	0
	Total de Riesgos	2	2
Seguridad	Extrema	1	2
	Alta	5	4
	Moderada	0	0
	Baja	0	0
	Total de Riesgos	6	6
Operación	Extrema	2	2
	Alta	10	7
	Moderada	0	2
	Baja	0	1
	Total de Riesgos	12	12
Gestión	Extrema	3	3
	Alta	12	15
	Moderada	6	2
	Baja	0	1
	Total de Riesgos	21	21
Recursos Humanos	Extrema	0	0
	Alta	2	1

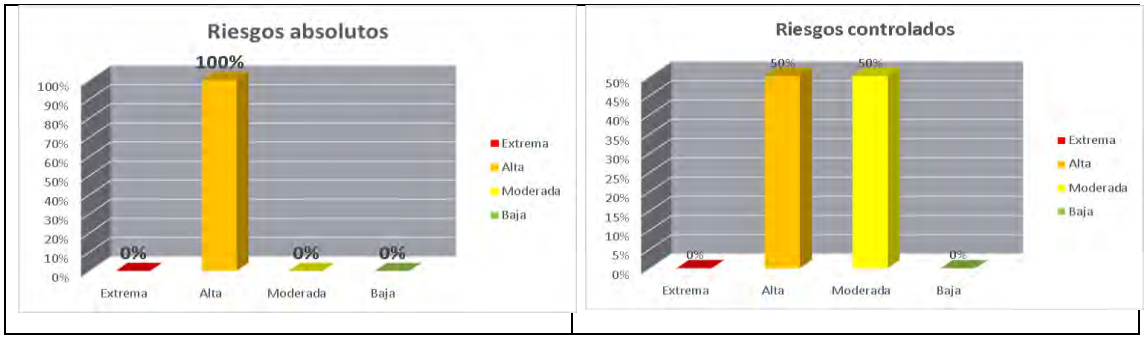
	Moderada	1	1
	Baja	0	1
	Total de Riesgos	3	3

Fuente: Elaboración propia

En la Tabla 4.15 se puede observar la evaluación de los riesgos, mediante gráficos, según cada proceso de TI, tanto a nivel absoluto como a nivel controlado. De esta manera se puede visualizar fácilmente el efecto de los controles en la distribución de los riesgos según su severidad la cual está representada en lo gráficos por los colores usados en los mapas térmicos.

Tabla 4. 15: Riesgos de Infraestructura

SEVERIDAD	RIESGOS ABSOLUTOS	RIESGOS CONTROLADOS
Extrema	0%	0%
Alta	100%	50%
Moderada	0%	50%
Baja	0%	0%

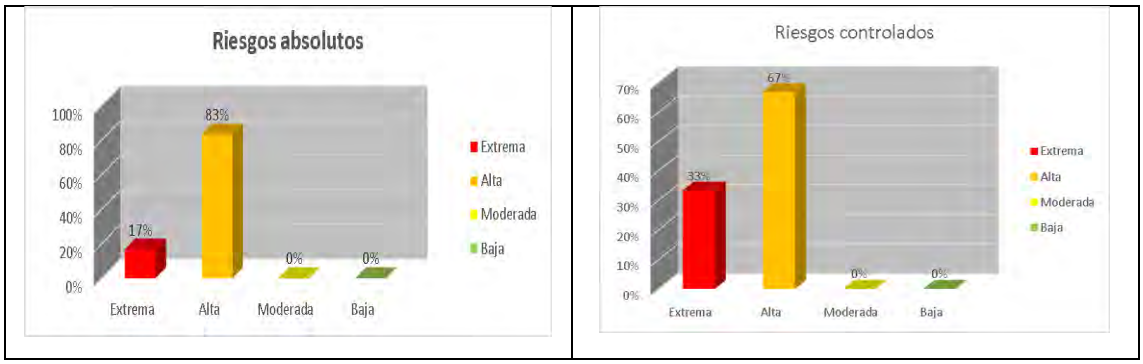


Fuente: Elaboración propia

Luego de realizar la valoración de riesgos absolutos, en el proceso de infraestructura, se tiene 2 riesgos que deben ser gestionados por su severidad alta, que representa el 100% de los riesgos identificados y relacionados con este proceso.

Tabla 4. 16: Riesgos de Seguridad

SEVERIDAD	RIESGOS ABSOLUTOS	RIESGOS CONTROLADOS
Extrema	17%	33%
Alta	83%	67%
Moderada	0%	50%
Baja	0%	0%

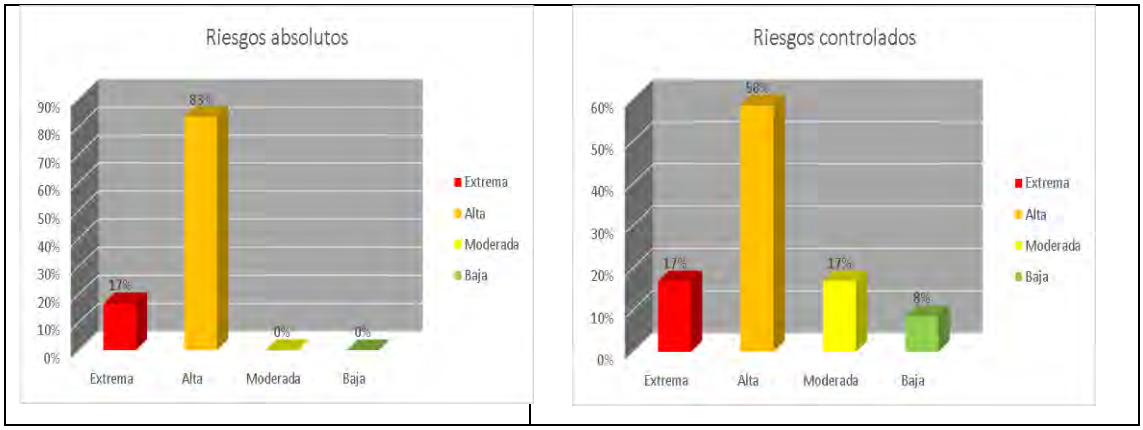


Fuente: Elaboración propia

Al realizar la valoración de riesgos de control, en el proceso de seguridad, se tiene 2 riesgos que deben ser gestionados por su severidad extrema que representa el 33% y otros 4 riesgos por su severidad alta que representa el 67% de los riesgos identificados y relacionados con este proceso.

Tabla 4. 17: Riesgos de Operación

SEVERIDAD	RIESGOS ABSOLUTOS	RIESGOS CONTROLADOS
Extrema	17%	17%
Alta	83%	58%
Moderada	0%	17%
Baja	0%	8%

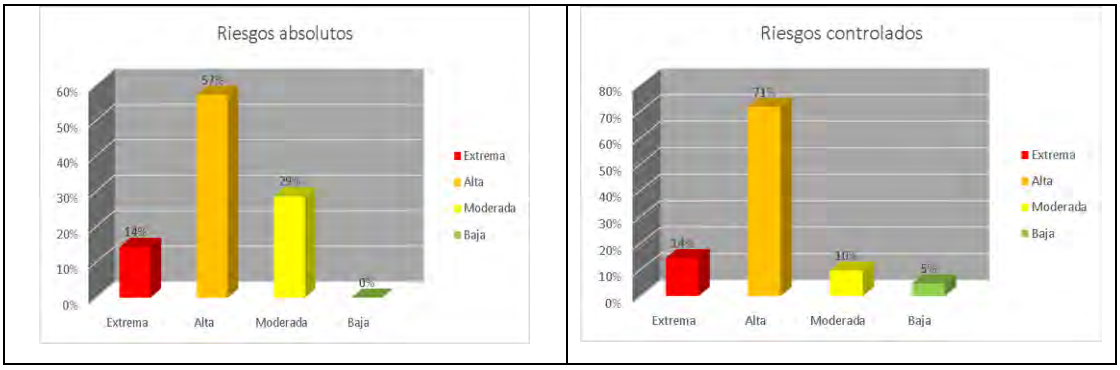


Fuente: Elaboración propia

En la calificación de riesgos controlados el 75% de los riesgos identificados de un total de 12 para el proceso de operación, se encuentran con calificación de severidad extrema o alta.

Tabla 4. 18: Riesgos de Gestión

SEVERIDAD	RIESGOS ABSOLUTOS	RIESGOS CONTROLADOS
Extrema	14%	15%
Alta	57%	71%
Moderada	29%	10%
Baja	0%	5%



Fuente: Elaboración propia

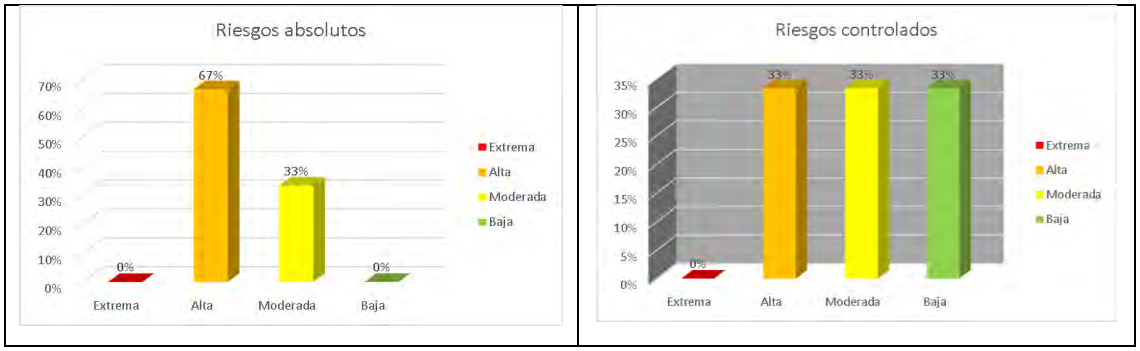
El mayor número de riesgos identificados están asociados con el proceso de gestión, de los 21 riesgos controlados 18 se encuentran en las categorías de severidad extrema y alta, por

lo que deben ser abordados cuidadosamente para su gestión correspondiente. Esos 18 riesgos representan el 85% de los riesgos identificados.

Los riesgos absolutos en la categoría de severidad extrema y alta llegan al 71%.

Tabla 4. 19: Riesgos de Recursos Humanos

SEVERIDAD	RIESGOS ABSOLUTOS	RIESGOS CONTROLADOS
Extrema	0%	0%
Alta	67%	33%
Moderada	33%	33%
Baja	0%	33%



Fuente: Elaboración propia

Con relación al proceso de recursos humanos se identificaron 3 riesgos absolutos, de los cuales el 67% corresponde a la categoría de severidad alta.

Asimismo, se hace conocer a la alta gerencia, sea esta pública y/o privada un conjunto de recomendaciones. Como caso práctico, para que un auditor informático pueda emitir opinión respecto al hallazgo aplicado al "INSTITUTO TECNOLOGICO MARCELO QUIROGA SANTA CRUZ" se propone:

1. Debilidades en las copias de respaldo

Condición

Como resultado de la visita realizada al "INSTITUTO TECNOLOGICO MARCELO QUIROGA SANTA CRUZ", verificamos que no se cumple con el procedimiento generalmente aceptado de copia de datos desde los ordenadores y/o servidores a cintas magnéticas y/o DVD´s.

Criterio

El procedimiento de copias de respaldo es parte del plan de seguridad. Específicamente relacionado a la seguridad lógica, donde debe detallar el procedimiento de copias de respaldo, en forma específica el procedimiento de copia de datos de los servidores a cintas magnéticas.

La ISO 27001 hace énfasis en que seguridad total es inalcanzable, pero mediante el proceso de mejora continua del sistema de seguridad se puede conseguir un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran.

La norma ISO 27001 e ISO 27002 en sus diferentes apartados relacionado a la seguridad como ser 8.3 "manejo de los soportes de almacenamiento", 8.3.3 "Soportes físicos en tránsito", 10.5.1 "Resguardo de la información", establece la necesidad de implementar normas y procedimientos de control que aseguren y garanticen el correcto tratamiento de la información de la institución.

Causa

Si bien se realizan actividades relacionadas a las copias de respaldo, no se habría analizado el riesgo de no cumplir con los procedimientos formalmente aprobados.

Efecto

El no seguir el procedimiento formalmente aprobado para la administración de las operaciones de IT incrementa el riesgo de que no se pueda restaurar datos a tiempo en casos de contingencias y que la continuidad de las operaciones se vea comprometida:

- Perder información de la empresa;
- Quiebra de la empresa;
- Romper la cadena de custodia.

Recomendación

Se deben realizar copias de respaldo de datos e información y de los programas fuente del sistema que contemple medios de almacenamiento, dispositivos, cantidad de copias a obtenerse, resguardo de las copias tanto en sitios seguros internos como externos, responsabilidad para la obtención, pruebas de recuperación para garantizar que las copias son utilizables, y se deben poner a prueba con regularidad de acuerdo con el Manual de Funcionamiento y Procedimientos formalmente aprobados.
Las copias realizadas deben verificarse que están correctas y además debe quedar registrada su ubicación, la cual debe ser distinta a la de la original para evitar que ambas se afecten por un mismo problema. Si se produjera algún incidente, los datos y programas afectados deben poder recuperarse mediante un proceso de restauración desde la copia de seguridad

Comentario de la Entidad:

Se tomará en cuenta la recomendación.

4.2.1.1.5. DEFINIR UN PORTAFOLIO DE ACCIONES PARA LA GESTIÓN DE RIESGOS

Para gestionar las oportunidades para reducir el riesgo debemos priorizar riesgos.

Riesgos prioritarios

Después de realizar el análisis de riesgos y determinar su nivel de severidad tanto en la calificación de riesgos absolutos como de riesgos controlados se puede observar en la Tabla 4.20 los riesgos que son de prioritaria atención:

Tabla 4. 20: Riesgos Prioritarios

NRO.	DETALLE DE RIESGO	PROCESO DE TI RELACIONADO
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Gestión
2	Desarrollar productos que no cumplen con las especificaciones.	Gestión
3	Desarrollar productos basados en requerimientos incorrectos.	Gestión
4	Versiones de software desactualizadas	Gestión
5	Adquirir software sin programas fuentes	Gestión
6	Equipo dañado no puede ser reparado	Operación
7	Red inalámbrica insegura	Operación
8	Obsolescencia de la infraestructura tecnológica	Gestión
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Gestión
10	No existe manual de usuario para el uso del sistema	Gestión
11	Se adquiere equipo no compatible con la infraestructura en uso	Gestión
13	Versiones de software para desarrollo y producción diferentes.	Operación
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Operación
15	Instalación de parches sin seguir las recomendaciones del proveedor	Seguridad
16	No existe contrato de mantenimiento	Gestión
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	Gestión
19	Suspensión de servicio de Internet	Infraestructura
21	Equipo de usuario final inseguro	Seguridad
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	Seguridad
23	No se conocen los costos asignados a los servicios prestados por TI	Gestión
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	Operación
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	Operación
29	Alteración o pérdida de la información registrada en base de datos o equipos.	Seguridad
30	Información desactualizada o incorrecta	Operación
31	Acceso no autorizado a la información	Seguridad
32	No aplicación de las políticas para la generación de respaldos	Operación
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	Gestión
35	No contar con la documentación de los procesos de TI	Gestión
36	Uso de software sin licencia	Seguridad
37	Se tiene Plan Estratégico desactualizado	Gestión
40	No se tiene dominio sobre las herramientas en uso	Recursos humanos
42	Desarrollar productos que no cumplen con los requerimientos de calidad	Operación
43	No administrar los riesgos de TI	Gestión
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	Gestión

Fuente: Elaboración propia

Planes de tratamiento

Para cada uno de los riesgos cuya evaluación de severidad, a nivel de riesgos controlados, fue de extrema o alta, se deben estimar tomando los planes de acción como se puede observar en la Tabla 4.21.

Tabla 4. 21: Planes de Acción

NRO.	DETALLE DE RIESGO	PLANES DE ACCIÓN
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Desarrollar políticas de gestión de requerimientos basados en necesidades institucionales.
2	Desarrollar productos que no cumplen con las especificaciones.	Documentos formalmente aprobados para la gestión de productos software
3	Desarrollar productos basados en requerimientos incorrectos.	Documentos formalmente aprobados basadas en necesidades institucionales
4	Versiones de software desactualizadas	Se presupuestaron las partidas para contratar el mantenimiento y se incluyó en el POA.
5	Adquirir software sin programas fuentes	Asegurar que por lo menos se tendrá el soporte necesario en caso de algunas contingencias
6	Equipo dañado no puede ser reparado	Contratar servicios de mantenimiento externo
7	Red inalámbrica insegura	Desarrollar una política de seguridad
8	Obsolescencia de la infraestructura tecnológica	Gestionar la baja de equipos
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Aplicar Interfaz gráfica de usuario amigable
10	No existe manual de usuario para el uso del sistema	Documentos formalmente aprobados para el uso del sistema
11	Se adquiere equipo no compatible con la infraestructura en uso	Desarrollar políticas de gestión de requerimientos basados en necesidades institucionales.
13	Versiones de software para desarrollo y producción diferentes.	Documentos formalmente aprobados para aplicar la ingeniería de software
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Desarrollar, revisar y/o actualizar la gestión de cambios
15	Instalación de parches sin seguir las recomendaciones del proveedor	Procedimientos formalmente aprobados para la modificación o mantenimiento del sistema
16	No existe contrato de mantenimiento	Documentos formalmente aprobados basadas en necesidades institucionales
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	Documentos formalmente aprobados basadas en necesidades institucionales
19	Suspensión de servicio de Internet	Cumplimiento a la política de seguridad y servicios
21	Equipo de usuario final inseguro	Cumplimiento a procedimientos de seguridad
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	Documentos formalmente aprobados para la gestión de cuentas de usuario
23	No se conocen los costos asignados a los servicios prestados por TI	Desarrollar, revisar y/o actualizar la gestión de cambios
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	Desarrollar, revisar y/o actualizar la gestión de cambios
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	Desarrollar, revisar y/o actualizar la gestión de cambios
29	Alteración o pérdida de la información registrada en base de datos o equipos.	Procedimientos formalmente aprobados para el diseño y mantenimiento de la base de datos
30	Información desactualizada o incorrecta	Documentos formalmente aprobados para la gestión de productos software
31	Acceso no autorizado a la información	Documentos formalmente aprobados para la gestión de cuentas de usuario
32	No aplicación de las políticas para la generación de respaldos	Procedimientos formalmente aprobados para las copias de seguridad de los datos y aplicaciones
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	Desarrollar planes de contingencia
35	No contar con la documentación de los procesos de TI	Documentos formalmente aprobados para la gestión de TI
36	Uso de software sin licencia	Aplicación de normas gubernamentales
37	Se tiene Plan Estratégico desactualizado	Documentos formalmente aprobados basadas en estratégias institucionales
40	No se tiene dominio sobre las herramientas en uso	Capacitación de recursos humanos
42	Desarrollar productos que no cumplen con los requerimientos de calidad	Documentos formalmente aprobados para aplicar la ingeniería de software
43	No administrar los riesgos de TI	Desarrollar planes de contingencia y gestión de riesgos
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	Capacitación de recursos humanos

Fuente: Elaboración propia

Evaluación de riesgos tratados

En Tabla 4.18 se presenta la calificación de los riesgos proyectando la aplicación de los planes de tratamiento (riesgos tratados):

Tabla 4. 22: Calificación de los Riesgos Proyectados

NRO.	DETALLE DE RIESGO	P	I	S
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	1	3	3
2	Desarrollar productos que no cumplen con las especificaciones.	1	2	2
3	Desarrollar productos basados en requerimientos incorrectos.	1	2	2
4	Versiones de software desactualizadas	2	3	6
5	Adquirir software sin programas fuentes	1	3	3
6	Equipo dañado no puede ser reparado	1	4	4
7	Red inalámbrica insegura	1	3	3
8	Obsolescencia de la infraestructura tecnológica	2	3	6
9	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	1	3	3
10	No existe manual de usuario para el uso del sistema	1	2	2
11	Se adquiere equipo no compatible con la infraestructura en uso	1	3	3
13	Versiones de software para desarrollo y producción diferentes.	1	4	4
14	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	1	3	3
15	Instalación de parches sin seguir las recomendaciones del proveedor	1	4	4
16	No existe contrato de mantenimiento	1	4	4
18	Recursos de la infraestructura tecnológica no son suficientes para atender demandas de servicios	1	4	4
19	Suspensión de servicio de Internet	1	5	5
21	Equipo de usuario final inseguro	1	2	2
22	Errores en la creación de usuarios y en la asignación de privilegios de acceso	1	2	2
23	No se conocen los costos asignados a los servicios prestados por TI	1	4	4
27	Se realizan cambios en la configuración de infraestructura y no se reflejan en la documentación	1	3	3
28	No se conoce el impacto de hacer cambios en los componentes de la configuración	1	4	4
29	Alteración o pérdida de la información registrada en base de datos o equipos.	1	3	3
30	Información desactualizada o incorrecta	1	3	3
31	Acceso no autorizado a la información	1	3	3
32	No aplicación de las políticas para la generación de respaldos	1	4	4
34	No contar con proceso para revisar el desempeño actual y la capacidad de los recursos de TI	1	4	4
35	No contar con la documentación de los procesos de TI	1	3	3
36	Uso de software sin licencia	2	3	6
37	Se tiene Plan Estratégico desactualizado	2	3	6
40	No se tiene dominio sobre las herramientas en uso	2	3	6
42	Desarrollar productos que no cumplen con los requerimientos de calidad	2	3	6
43	No administrar los riesgos de TI	1	4	4
44	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos	1	5	5

Fuente: Elaboración propia

4.2.1.1.6. RESPONDER AL RIESGO

Con la finalidad de contar con instituciones o entidades adecuada para la Gestión de los Riesgos, y con el objetivo de mantener riesgos actualizados, controlados, y planes de tratamiento para mitigarlos. Se debe gestionar los recursos humanos, para asignar responsabilidades a personas que cumplan el rol de recopilación de riesgos en un nivel preliminar, los procese, y para que actualice el mapa térmico para conocimiento de la alta gerencia.

La identificación y evaluación de los riesgos debe ser sustentado por un sistema participativo de planificación que considere la misión y la visión institucionales, así como objetivos, metas y políticas.

Los documentos para la identificación de riesgos estarán basados principalmente en los siguientes:

- Políticas y objetivos estratégicos institucionales;
- Análisis exhaustivo del entorno interno y externo;
- Evaluaciones institucionales en forma periódica;
- Normativa externa e interna asociada con los procesos;
- Documentos de operación diaria y de la evaluación periódica.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Este modelo permite gestionar los riesgos relacionados a TI y tomar las acciones preventivas, detectivas y correctivas adecuadas con el fin de minimizar los diferentes tipos de riesgos. El modelo esta adecuado a la realidad de nuestro país.

Es importante resaltar que cada vez que se incorpora una nueva herramienta o negocio de TI a la entidad se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos.

El modelo propuesto, contribuye a fomentar las actividades de TI, posicionando la imagen institucional y generando confianza frente a terceros.

- La metodología propuesta, cumple con los objetivos planteados;
- La gestión responsable de riesgos se basa en las personas;
- Las personas que cumplan el rol de gestor de riesgos podrán utilizar el presente modelo y aplicar los controles que considere necesario en forma sistemática y disciplinada;
- La gestión de riesgo tecnológico es una de las responsabilidades y desafíos más importantes a las cuales se enfrentan las entidades públicas y privadas, debido a que involucra el uso de recursos organizacionales, humanos, financieros y tecnológicos;
- Es posible adaptar un marco de trabajo para la gestión de riesgos de TI, basado en mejores prácticas como COBIT 5 y mapear con otros estándares;
- El rol del Contador Público debe evolucionar de tal forma que se convierta en un factor importante dentro de la evaluación del riesgo tecnológico y en la mejora continua de los procesos de TI, a través del uso de herramientas tecnológicas para

el análisis de las operaciones, la evaluación de riesgos y la planificación de la auditoría.

5.2. RECOMENDACIONES

Teniendo como base el análisis de gestión de riesgos, se detallan las siguientes recomendaciones generales:

- Mantener un mapa térmico actualizado con los riesgos controlados que están identificados con una severidad alta o extrema;
- Desarrollar reuniones permanentes de altos ejecutivos con los responsables de la gestión de riesgos para la evaluación de los planes de tratamiento que se están aplicando a los riesgos del mapa térmico identificados como alto o extremo, con el objetivo de actualizarlos si se considera que es factible mejorarlos para mitigar el riesgo;
- Fortalecer la gestión de riesgos, mediante capacitación permanente;
- Centralizar la actualización preliminar de los riesgos identificados, controlados, y planes de tratamiento, en un responsable designado por la alta gerencia, que estará a cargo de preparar el material para reuniones y alertar a la unidad que corresponda inmediatamente, en caso de que se detecte un nuevo riesgo que clasifique como alto o severo;
- Capacitar al responsable para que procese los nuevos riesgos con fines de clasificarlos, para alertar a la jefatura en caso de riesgos extremos o altos y mantener la gestión de riesgos actualizada;
- Desarrollar y/o adquirir un sistema que facilite la administración basada en riesgos;
- En futuros trabajos, sería interesante rescatar las mejores de prácticas inherentes a la gestión de riesgos de TI como: ISO 20000, ISO-27001, ISO-27005, ISO 31000, MAGERIT, ITIL, COSO y generar un modelo y/o método mapeando con estos estándares para agregar valor a la empresa o institución.

REFERENCIAS BIBLIOGRÁFICAS

[ARIAS 2005] ARIAS RUIZ DE SOMAVIA, RAMÓN; Análisis de Riesgos del Sistema de Información clasificado de Isdefe. Informe interno de la empresa. 2005.

[Ernst 2012] Ernst & Young, "Cambios en el panorama de los riesgos de TI," 2012.

[ISACA 2012] ISACA, COBIT 5. Procesos Catalizadores. Rolling Meadows, Illinois, 2012.

[ISACA 2013] ISACA, COBIT 5 for Risk. 2013.

[MONJE 2011] MONJE ALVAREZ, CARLOS ARTURO; Metodología de la Investigación Cuantitativa y Cualitativa. 2011.

[Ramírez 2011] A. Ramírez and Z. Ortiz, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," Ingeniería, vol. 16, no. 2, pp. 56–66, 2011.

[Hernández 2005] Hernández, R., 2005: Metodología de la Investigación, 505 pp. Editorial McGraw-Hill.

En línea:

[Acceso, junio 2017] Riesgos y seguridad en los sistemas de información. Auditoría informática.
http://ciberconta.unizar.es/LECCION/SEGURO/inicio.html

[Acceso, Febrero 2017] ISACA-ITGI. (2016). *isaca.org/ITGI*. (I. G. Institute, Productor) de IT Governance Institute:
http://www.isaca.org/spanish/Pages/default.aspx

[Acceso, Febrero 2017] COSO. *Committee Of Sponsoring Organizations of the treadway commission.* Welcome to COSO:
https://www.coso.org/Pages/default.aspx

[Acceso, Diciembre 2016] Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Practicas TI en cumplimiento de la Ley Sarbanes–Oxley *http://www.revistaespacios.com/a17v38n23/17382303.html*

[Acceso, Diciembre 2017] Norma Técnica Colombiana NTC-ISO/IEC 27005. *https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf*

[Acceso, Octubre 2017] Gestión del Riesgo ISO 31000. *https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/*

[Acceso, Enero 2018] Norma Internacional ISO 31000. *http://gestion-calidad.com/wp-content/uploads/2016/09/iso_31000_2009_gestion_de_riesgos.pdf*

[Acceso, Noviembre 2018] COBIT 5 aplicado al sistema de registro contable informático argentino *http://www.isaca.org/COBIT/focus/Pages/COBIT-5-Applied-to-the-Argentine-Digital-Accounting-System-Spanish.aspx*