VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN DE LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS
II PROMOCIÓN

TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

TEMA: "PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS EN EMPRESAS PROVEEDORAS DE SERVICIOS DE TELECOMUNICACIONES"

AUTORES:
RUBÉN VINICIO FERNÁNDEZ MATUTE
NELSON GUSTAVO MONTEROS MONTENEGRO

DIRECTOR: ING. PAULO BERMEO MSC.

SANGOLQUÍ, NOVIEMBRE DE 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

CERTIFICADO

ING. PAULO BERMEO MSc.
Director

ING. VICENTE MERCHÁN R. MSc.
Oponente

CERTIFICAN

Que el trabajo titulado "PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS EN EMPRESAS PROVEEDORAS DE SERVICIOS DE TELECOMUNICACIONES.", realizado por el Ing. Rubén Vinicio Fernández Matute y el Ing. Nelson Gustavo Monteros Montenegro, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Debido a que se ha cumplido con las normas estatuarias establecidas por la ESPE para el desarrollo del trabajo de conclusión de carrera, se recomienda su publicación.

El mencionado trabajo consta del documento empastado y disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf).

Sangolquí, Noviembre de 2014

ING. PAULO BERMEO MSc.
Director

ING. VICENTE MERCHÁN R. MSc.
Oponente

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
II PROMOCIÓN

DECLARACIÓN DE RESPONSABILIDAD

Rubén Vinicio Fernández Matute
Nelson Gustavo Monteros Montenegro

DECLARAMOS QUE:

El proyecto de Maestría denominado "PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS EN EMPRESAS PROVEEDORAS DE SERVICIOS DE TELECOMUNICACIONES", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el trabajo correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de Maestría en mención.

Sangolquí, Noviembre de 2014

_____ _____

Ing. Rubén Vinicio Fernández Matute Ing. Nelson Gustavo Monteros Montenegro

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE
VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
II PROMOCIÓN

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Rubén Vinicio Fernández Matute y Nelson Gustavo Monteros Montenegro

Autorizamos a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la Institución, del trabajo "PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS EN EMPRESAS PROVEEDORAS DE SERVICIOS DE TELECOMUNICACIONES", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Noviembre de 2014

_____	_____
Ing. Rubén Vinicio Fernández Matute	Ing. Nelson Gustavo Monteros Montenegro

DEDICATORIA

A las mujeres de mi vida, mi querida esposa que con todo su amor y paciencia ha sabido darme sus palabras de aliento en cada momento, de igual forma a mis dos hijas Nathaly y Melissa que soportaron las ausencias de su padre, este logro para ustedes dedicado con todo mi amor.

A mis padres por sus enseñanzas de esfuerzo y responsabilidad, de igual forma a mis hermanos por brindarme todo su apoyo incondicional en el transcurso de esta Maestría.

Rubén Vinicio Fernández M.

DEDICATORIA

A mis padres y hermanos por su apoyo incondicional, por enseñarme el valor del esfuerzo y responsabilidad.

Nelson Gustavo Monteros M.

AGRADECIMIENTO

Nuestro más amplio agradecimiento para el Ing. Paulo Bermeo por su valiosa orientación y apoyo, quién con su excelente respaldo e interés, hicieron posible la realización de este trabajo.

Nuestra gratitud a la Universidad de las Fuerzas Armadas (ESPE), por el gran aprendizaje mediante experiencias y conocimientos impartidos.

De la misma manera nuestro agradecimiento al Ing. Vicente Merchán por las valiosas aportaciones y recomendaciones.

A nuestro estimado amigo Ing. Hugo Vecino, por su guía y respaldo en la ejecución de este proyecto.

Gracias al apoyo de la Superintendencia de Telecomunicaciones y a los proveedores de servicio de Internet (ISP) que accedieron a la encuesta planteada; de manera especial a la empresa que nos brindó su total apertura al participar en la aplicación de la propuesta metodológica desarrollada.

Rubén Vinicio Fernández M.

Nelson Gustavo Monteros M.

ÍNDICE DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

RESUMEN

El presente proyecto tiene por objetivo establecer una propuesta metodológica para gestionar los riesgos tecnológicos en empresas Proveedoras del Servicio de Internet (ISP). Ésta nace de una investigación previa realizada al sector, en empresas autorizadas a operar y brindar el servicio en la ciudad de Quito, para lo cual, se tomó como referencia el estándar internacional de control: COBIT 4.1. Como resultado se determinó un nivel relativamente bajo de madurez con el que dichas empresas gestionan los riesgos de Tecnologías de la Información. Adicionalmente, los análisis de otros marcos de referencia como: MAGERIT v3, ISO/IEC 27005: 2012 y las Guías de Auditoría de Tecnología Global GTAG, son otro punto importante en el desarrollo de la metodología propuesta; la misma que una vez definida y estructurada se aplicó a un ISP representativo de la ciudad de Quito. Esta aplicación permitió contar con información real para cada fase, actividad y tarea del proyecto; y a su vez posibilitó el identificar un escenario de riesgo en base a los diferentes activos tecnológicos y procesos propios de dicha empresa, efectuando el respectivo análisis y evaluación de dichos riesgos. Por tanto, el primer resultado del proyecto es una propuesta metodológica aplicable a cualquier empresa proveedora de servicios de telecomunicaciones, ajustada a un entorno y variables locales; y el segundo corresponde a una matriz de riesgos priorizados de beneficio exclusivo para la empresa del caso de estudio; así como el correspondiente informe puesto a disposición de la Gerencia con los controles que se consideraron más adecuados.

PALABRAS CLAVE: COBIT, MAGERIT 3.0, GTAG, GESTIÓN DE RIESGOS DE TI, NIVEL DE MADUREZ, ISP, TELECOMUNICACIONES.

ABSTRACT

This project aims to establish a methodology for managing technological risks in Internet Service Providers (ISP). It born from a previous research on the sector such authorized to operate and provide services in Quito companies to which reference was made to international standard COBIT 5. As a result, a relatively low level of maturity was determined with which these companies manage their risks of Information Technology. Additionally, the analysis of other frameworks such as: MAGERIT v3, ISO / IEC 27005: 2012 and GTAG is another important development point of the proposed methodology that once it was defined and structured it was applied on a representative ISP of Quito. This application allow to have real information for each phase, activity and task in the project; and in turn made it possible to identify a risk scenario based on different proprietary processes and technology assets of the company, making the respective analysis and evaluation of such risks. Therefore, the first results of the project is a proposed methodology applies to any provider of telecommunications services, adjusted to an environment and local variables; and the second corresponds to a matrix of prioritized risks with the exclusive benefit for the company of the case study and the report available to the management with the most appropriate surveys for managing each risk.

KEY WORDS: COBIT, MAGERIT 3.0, GTAG, TI MANAGEMENT RISK, ISP, MATURITY MODEL, TELECOMMUNICATIONS.

CAPITULO I

MARCO CONCEPTUAL

1.1. Introducción

En Ecuador y en varias otras regiones del mundo, las telecomunicaciones son consideradas un sector estratégico en la economía por el papel fundamental que tienen en los campos de investigación y desarrollo y por su directa influencia en el marco competitivo del aparato productivo de un país. Bajo ese contexto, las TELCO[1] se encuentran "obligadas" a integrar de manera adecuada y eficiente sus actividades de negocio con la constante innovación tecnológica a efectos de cubrir satisfactoriamente los demandantes requerimientos de calidad y oportunidad de un sector tan importante.

Esta integración requiere de cambios e implementaciones que evidentemente a su vez conllevan riesgos tecnológicos y amenazas que no pueden pasarse por desapercibidos para el cumplimiento del objetivo del negocio de la empresa. Éste es un tema muy sensible en empresas proveedoras de servicios de telecomunicaciones en las que los SLA[2] suscritos con sus clientes las comprometen a alcanzar elevados índices de disponibilidad, mismos que podrían lograrse con una apropiada identificación y control de aquellas situaciones que amenacen la continuidad de la provisión del servicio.

1.2. Estado del arte

1.2.1. A nivel mundial y local

El trabajo de investigación propuesto busca obtener un panorama general del nivel y madurez con el cual las empresas proveedoras de Internet en la ciudad de Quito administran sus riesgos tecnológicos. Sobre esa base, se plantea el desarrollo de una propuesta metodológica para la gestión de riesgos tecnológicos de dicho

[1]TELCO, nombre genérico utilizado para denominar a una empresa de telecomunicaciones.

[2]SLA: Service Level Agreeement. Acuerdo de nivel de servicio suscrito entre un proveedor de servicios y su cliente.

sector; y, posteriormente ensayarla sobre una empresa de este tipo en particular para contribuir con recomendaciones y estrategias de mitigación.

The Ernst & Young Business Risk Report 2010, en su publicación "**The top 10 risks for global business"**, menciona que el entorno empresarial actual es un constante desafío que trae consigo nuevos horizontes de riesgo para empresas que, a nivel mundial, se enfrentan a cambios producidos por una economía post-recesión. Los autores manifiestan que la capacidad de anticiparse a las amenazas, responder y adaptarse continuamente es un elemento crítico en el proceso de gestión de riesgos. En virtud de lo cual, recopilaron las opiniones y experiencias de empresas pertenecientes a 14 sectores industriales (entre ellos, telecomunicaciones), alcanzado un panorama general del impacto de los riesgos en cada sector para luego identificar los 10 principales riesgos a los cuales se encuentra expuesta una organización.

The Institute of Internal Auditors, en su guía de auditoría **"Global Technology Audit Guide: Developing de IT Auditing Plan"** manifiesta que para una organización resulta de vital importancia determinar el contenido de su portafolio de riesgos e implementar actividades encaminadas a administrar dichos riesgos hacia un nivel aceptable. De acuerdo a esta guía, una adecuada evaluación del riesgo debe examinar la infraestructura, aplicaciones y componentes que representen la mayor amenaza para la capacidad de la organización para asegurar la disponibilidad del sistema; y la fiabilidad, integridad y confidencialidad de los datos.

Infogex Ltda., empresa colombiana especializada en seguridad de la información, en su documento **"Procedimiento de análisis y valoración de riesgo para un Sistema de Información"** ejecuta la estandarización de un método de análisis y valoración de riesgo para un sistema de información. A través de dicho procedimiento, los autores proponen la identificación de los procesos de negocio de una organización para distinguir los activos del Sistema considerando toda la infraestructura tecnológica, organizacional y humana para describir las amenazas potenciales que pueden causar incidentes de seguridad.

Por otra parte, si bien a nivel local no se han encontrado trabajos de investigación que se encuentren relacionados directa y específicamente a la evaluación y administración de riesgos en el sector de las telecomunicaciones; es importante destacar el estudio publicado por **Katalina Coronel Hoyos** quien presenta una metodología de evaluación del riesgo tecnológico en las instituciones del sistema financiero ecuatoriano utilizando COBIT 4.1 basada en modelos de madurez para la evaluación de los procesos de tecnología de la información.

La metodología desarrollada por la autora determina los requerimientos normativos de tecnología de información para las instituciones controladas por la Superintendencia de Bancos y Seguros; luego, establece los objetivos de control de COBIT 4.1 que los satisfacen y verifica la eficiencia de la metodología mediante su aplicación en una institución financiera.

1.2.2. Proveedores de servicios de Internet

En el Ecuador y en varias otras regiones del mundo existen varios grupos empresariales dentro del sector de las telecomunicaciones cumpliendo un rol fundamental en el desarrollo de la sociedad, economía e investigación.

Las TELCO se encuentran “obligadas” a integrar de manera adecuada y eficiente sus actividades de negocio con la constante innovación tecnológica a efectos de cubrir satisfactoriamente los demandantes requerimientos de calidad y oportunidad de un sector tan importante.

Dentro de estos grupos empresariales se encuentran aquellas empresas dedicadas a proveer específicamente el servicio de Internet, conocidas por sus siglas en inglés como ISP[3]. Los ISP son organizaciones cuyo objetivo fundamental es ofrecer a sus abonados y usuarios acceso a Internet y a sus servicios relacionados (registro de dominios, hosting, etc.) a través de diferentes tecnologías de última milla: Acceso vía

[3]ISP (Internet Service Provider), Proveedor de Servicio de Internet.

fibra óptica, vía cobre, vía radio; y, redes híbridas fibra – coaxial, principalmente. Para ello, un ISP debe procurar dos factores básicos que son:

- El establecimiento de la conectividad entre sus usuarios y la red de Internet; y,
- Alta disponibilidad del servicio.

Es decir, confirmada la conexión entre el usuario y la red de Internet, el ISP debe estar en la capacidad de mantener dicha conexión (en el segmento de red que es de su responsabilidad) dentro de los niveles de calidad y disponibilidad establecidos en los Acuerdos de Niveles de Servicios (SLA). Así, el cliente puede mantener conexión a diferentes redes a nivel mundial y acceso a cualquier servicio disponible en Internet como el WWW, transferencia de archivos (FTP), correo electrónico (SMTP), boletines electrónicos, mensajería instantánea (chats), servicios multimedia, transmisión de archivos, etc.

A continuación se detalla un diagrama esquemático de la situación de un Proveedor de Internet:

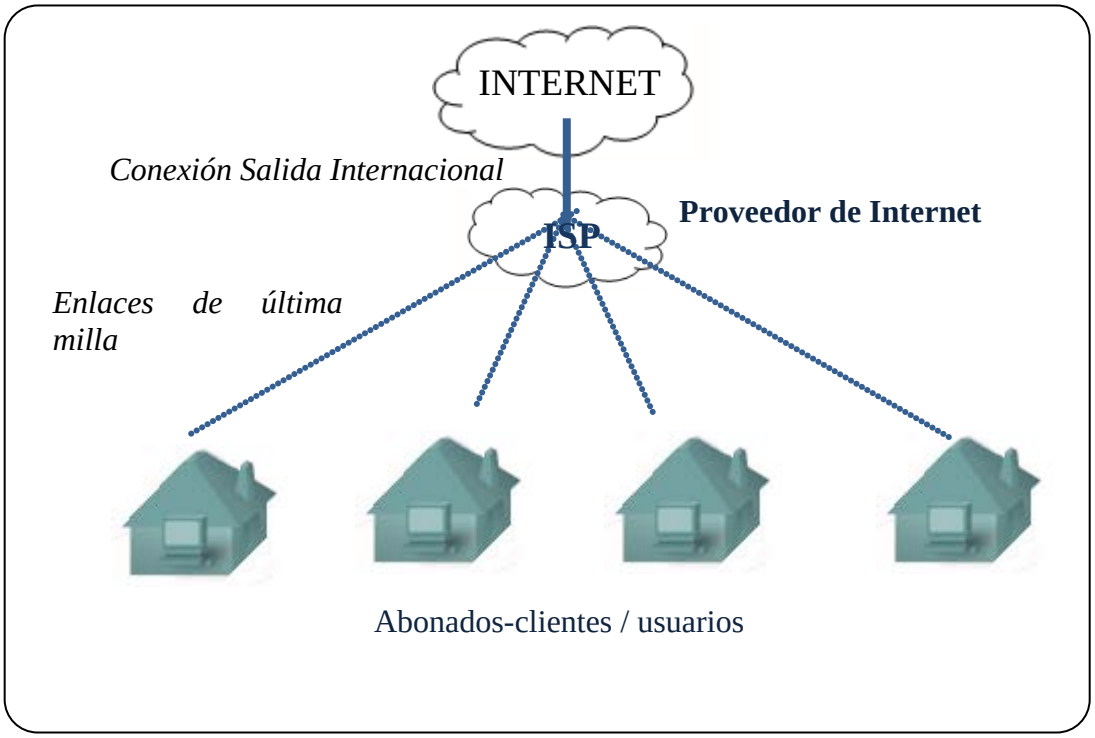


Figura 1 Diagrama esquemático de un ISP

Debiéndose destacar principalmente: A). La conexión entre el ISP a la red de Internet; y, B). El canal de acceso entre el cliente y el ISP, los cuales se detallan a continuación:

a) CANAL ISP – INTERNET: CONEXIÓN DE SALIDA INTERNACIONAL. Corresponde al canal de salida que el proveedor de Internet ISP contrata con empresas denominadas "carriers" o de servicio portador. Los denominados carriers son operadores de telecomunicaciones propietarios de las redes troncales de Internet y responsables del transporte de los datos. Por lo tanto, proporcionan conexión a Internet a alto nivel.

b) CANAL DE ACCESO CLIENTE – ISP: ENLACES DE ÚLTIMA MILLA. La última milla es la conexión entre el usuario final y el nodo o central que provee el servicio de Internet. Ésta puede corresponder a diversas tecnologías, las cuales dependerán esencialmente de su disponibilidad, costos, el dispositivo de acceso utilizado, los medios utilizados y la velocidad de la conexión. En todo caso, pueden considerarse cuatro modalidades de acceso principales:

- **Redes de acceso vía fibra óptica:** dependiendo del punto hasta el cual se extiende la fibra óptica desde el ISP (FTTx):

    - FTTH (Fiber to the home): fibra hasta el hogar del cliente.
    - FTTC (Fiber to the cabinet): fibra hasta el armario de distribución más cercano al usuario.
    - FTTB (Fiber to the building): fibra hasta la acometida del edificio.

- **Redes de acceso vía cobre:** el grupo de tecnologías de comunicación xDSL (Digital Subscriber Line) permite la transmisión de datos a mayores velocidades y vía modem, a través del par de cobre tradicional del servicio telefónico. Entre ellas se pueden citar:

- ADSL (Línea de Abonado Digital Asimétrica): la velocidad de descarga y de subida de datos no coinciden.
- SDSL (Línea de Abonado Digital Simétrica): misma velocidad de descarga y de subida.
- HDSL (Línea de abonado digital de alta velocidad binaria): para operar con tráfico de datos en forma digital bajo velocidades simétricas.

- **Redes de acceso vía radio:** Los clientes usan señales de radio en reemplazo del cobre, ideal para un despliegue rápido de red.

  - WLL (Wireless Local Loop, ó bucle local inalámbrico): enlace de comunicación inalámbrica punto a multipunto. Si bien puede operar en "bandas libres" (2.4 GHz y 5.7 – 5.8 GHz), éstas se descartan a efectos de evitar riesgos de saturación e indisponibilidad de la red. Esta tecnología generalmente es implementada en la banda de 3.5 GHz (banda licenciada).

  - LMDS (Local Multipoint Distribution Service): sistema de comunicación punto – multipunto inalámbrico. Trabaja en el margen superior del espectro electromagnético, de los 22 a los 42 GHz. En Ecuador, el rango de espectro asignado para servicios LMDS corresponde a la banda Ka: 27,5 GHz – 28,35 GHz; 29,1 GHz – 29,25; y en la banda de 31 GHz: 31,0 GHz – 31,3 GHz.

  - Broadband Wireless: utilizan sistemas de microondas de tipo punto (nodo o central) a multipunto (usuarios).
    MMDS: opera en las bandas 2,5 GHz a 2,9 GHz. (no licenciadas)
    LMDS: opera por encima de los 20 GHz en banda licenciada.

  - Sistemas celulares: para servicios de Internet móvil sobre tecnologías del servicio celular: LTE (4G), HSPA+ (3.5G), WCDMA (3G), GSM (2G), CDMA.

- **Redes híbridas fibra-coaxial (HFC):** redes de acceso que emplean fibra óptica en su segmento central y cable coaxial en las inmediaciones del usuario final.

Por otra parte, muchos ISP ofrecen servicios adicionales como por ejemplo cuentas de correo electrónico, exploradores web y espacios para crear y albergar un sitio web propio (filtrados, bloqueos, contenidos). Dichos servicios son implementados en un grupo de servidores que forman parte de la red interna del ISP.

1.2.2.1. Estructura de un ISP

Un ISP está conformado, de manera general, como se muestra a continuación:

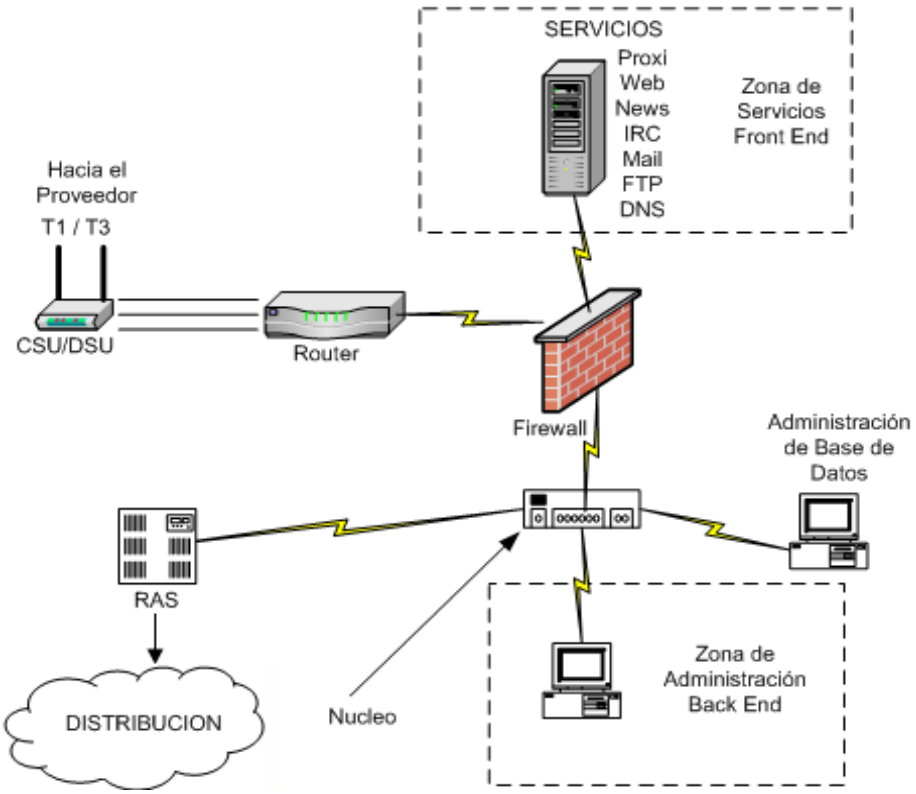


Figura 2. Estructura de un ISP

Se distingue el canal de salida internacional representado por la interfaz *CSU/DSU (Channel Service Unit/Data Service Unit)* que cumple las funciones de un módem externo para el intercambio de información entre una red LAN (ISP) y una

WAN (carrier). Por su parte, el segmento de acceso a clientes se esquematiza con el proceso de distribución (posterior a la autenticación de clientes ejecutada por el Servidor de Acceso Remoto RAS).

En lo que a seguridad se refiere, un elemento primordial es el ***firewall*** como un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Es un mecanismo para restringir el acceso entre la Internet y la red corporativa interna; y reduce las probabilidades de ataques externos a los sistemas corporativos y redes internas, además que puede servir para evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información peligrosa (como passwords no encriptados o datos sensitivos para la organización) hacia el mundo externo.

Por otra parte, debido a que para un ISP resulta primordial controlar los canales de comunicación de la red para que las peticiones de los usuarios conecten con la red de una posición remota; éste debe implementar un ***Servidor de Acceso Remoto*** (RAS, por sus siglas en inglés) que además le permite reconocer peticiones de la red y realizar la autenticación de clientes.

Adicionalmente, de la Figura 2, resulta importante destacar las dos estructuras funcionales fundamentales de un ISP:

- Administración; y,
- Servicios.

En la zona de administración se ejecuta la gestión del sistema de información y de servicios. Corresponde al back-end de la empresa, por lo que de cierto modo se encuentra oculta del usuario final y solo puede ser gestionada por el cliente intermedio o el administrador. Desde el punto de vista de seguridad, esta zona es la más importante a proteger puesto que las estaciones que pertenecen a la misma están en facultad de ingresar y controlar toda la plataforma del ISP.

Por su parte, la zona de servicios es el front-end del proveedor de Internet; es decir, el segmento que recepta las solicitudes y requerimientos de sus usuarios para acceder a un determinado servicio.

Por su naturaleza, la zona de servicios de un ISP se implementa sobre lo que se conoce como una Zona Desmililitarizada (DMZ) que corresponde a una red local ubicada entre la red interna del ISP y la red externa Internet. Una DMZ permite conexiones desde la red interna a la externa, mientras que las conexiones desde la DMZ sólo son posibles a la red externa. Es decir, los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Esta situación conlleva a que en la DMZ se puedan ubicar servidores que es necesario que sean accedidos desde fuera (como servidores de e-mail, Web y DNS). En ese sentido, estos servidores puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de intromisiones a la seguridad. En otras palabras, asegura que a la red interna únicamente llegan conexiones de la DMZ

1.2.2.2. Consideraciones generales sobre ISP

Cobertura.- Los ISP poseen cobertura definida; ya sea por regulación o por las condiciones del mercado. En el Ecuador, la cobertura de un ISP no puede exceder las zonas y/o ciudades específicamente establecidas en sus respectivos permisos de prestación de servicios.

Ancho de banda.- Comúnmente conocido como la velocidad de conexión que ofrece el ISP. Técnicamente, en enlaces no dedicados, este ancho de banda se comparte entre el número de suscriptores que se encuentren conectados simultáneamente, de modo que cuanto más aumenta el número de suscriptores, menor es la velocidad efectiva en el canal de acceso. Es importante mencionar que en el Ecuador, la normativa define que la transmisión de datos a una tasa igual o superior a 256 Kbps puede considerarse comercialmente como servicios de “Banda Ancha”.

Precio.- Este factor depende estrictamente del modelo de negocio, gestión y tecnología del ISP. En el Ecuador las tarifas de los servicios provistos por los ISP las regula el mercado.

Accesibilidad.- Depende también del modelo de negocio aplicado por cada ISP. Algunos ofrecen paquetes donde se considera el tiempo de conexión; es decir, no se puede exceder un cierto número de horas de conexión por mes. Otros por su parte, ofertan paquetes en los que se tasa el consumo de datos descargados (MB generalmente); y, otros proveedores incluso brindan servicios sin suscripción (bajo demanda).

A la diversidad de modelos se añaden las distintas posibilidades de aplicación de planes controlados, abiertos o servicios pre-pagados, que le permiten al ISP elaborar propuestas que puedan ser dirigidas a diferentes grupos de usuarios.

Servicios complementarios.- La competitividad del mercado en la provisión del servicio de Internet impone fuertes exigencias a las empresas ISP; adicionales a las que por regulación deben cumplir. Es fundamental para un ISP contar con:

- Acuerdos de niveles de servicios (SLA) con sus clientes.
- Acuerdos de niveles de servicios con proveedores.
- Cuadrillas de servicio técnico y Call Center (24/7)
- Centro de control de la red (NOC, Network Operations Center).
- Sistemas de gestión de usuarios.
- Sistemas de gestión de reclamos y averías.
- Departamentos de venta y servicios post-venta; entre otros.
- Brindar servicios de gerenciamiento de hosting, implementación de seguridad perimetral

1.2.2.3. Regulación vigente en Ecuador relacionada a las empresas proveedoras de servicios de valor agregado, modalidad Internet (ISP).

En lo que a telecomunicaciones respecta, en el Ecuador se mantiene vigente la Ley Especial de Telecomunicaciones Reformada y su correspondiente Reglamento General[4]; en el cual las empresas proveedoras del servicio de Internet ISP se reconocen como "Permisionarios para la explotación de Servicios de Valor Agregado modalidad Internet". La regulación del sector de las telecomunicaciones en el país está a cargo del Consejo Nacional de Telecomunicaciones CONATEL; organismo facultado para la expedición de normas y reglamentos de cumplimiento obligatorio para las diferentes operadoras de servicios de telecomunicaciones.

Por su parte, el control técnico al cumplimiento de la normativa establecida lo ejerce la Superintendencia de Telecomunicaciones, SUPERTEL, como organismo autónomo encargado de vigilar y auditar la prestación de los servicios de telecomunicaciones.

En lo relacionado específicamente a la prestación del servicio de Internet (Servicios de Valor Agregado, modalidad Internet) es de fundamental importancia mencionar la Resolución 216-09-CONATEL-2009 suscrita el 27 de julio de 2009 mediante la cual el Consejo Nacional de Telecomunicaciones aprobó los parámetros técnicos de calidad y las obligaciones que los proveedores del servicio de Internet deben cumplir. A continuación se resumen brevemente cada uno de estos parámetros de calidad:

Relación con el cliente.- Grado de satisfacción que tiene un usuario o cliente con respecto a su percepción del trato brindado por el ISP en términos de amabilidad, disponibilidad y rapidez.

---

[4] Decreto 1790 (Registro Oficial 404, 4-IX-2001); y, Decreto 2727 (Registro Oficial 599, 18-VI-2002).

Porcentaje de reclamos generales procedentes.- Porcentaje de reclamos generales procedentes realizados por los clientes con respecto al total de clientes en servicio, en el mes.

Tiempo máximo de resolución de reclamos generales.- Tiempo medido en horas continuas, que los clientes esperan para que su reclamo procedente reportado en cualquier punto de contacto del proveedor del servicio sea resuelto o atendido.

Porcentaje de reclamos de facturación.- Porcentaje de reclamos generales procedentes realizados por los clientes debido a posibles errores en la facturación, respecto al total de facturas emitidas, en un mes.

Tiempo promedio de reparación de averías efectivas.- Tiempo promedio medido en horas continuas que tarda en repararse una avería efectiva, medida desde el momento en que se produce el reclamo y se notifica al proveedor del servicio hasta la reparación de la misma.

Porcentaje de módems utilizados.- Porcentaje de módems utilizados respecto del total de módem que dispone el proveedor de Internet para efectuar conexiones conmutadas.

Porcentaje de reclamos por la capacidad del canal de acceso contratado por los clientes.- Porcentaje de reclamos procedentes relacionados con el ancho de banda real provisto en ambos sentidos del enlace (ascendente y descendente) no menor al 96% con respecto al ancho de banda contratado.

En cuanto a las obligaciones estipuladas en la Resolución en referencia se tienen:

- Informar al cliente sobre la relación efectiva de compartición del canal, disponibilidad y ancho de banda.
- Promocionar y publicitar correctamente sobre las condiciones de prestación de servicios de telecomunicaciones.

- Establecer mecanismos para que los usuarios accedan a Internet a través de tarjetas prepago.
- No bloquear o limitar el acceso o el uso de aplicaciones sin el consentimiento del usuario.
- Informar el cliente sobre las características de seguridad al intercambiar información.
- Informar al usuario de los derechos que le asisten.
- Disponer de procedimientos de gestión y atención de usuarios.
- Compromiso de reportar a la SUPERTEL y SENATEL.
- Habilitar en la página web de la empresa, vínculos al sitio web de la SUPERTEL.

1.3. Justificación e importancia

La justificación del presente estudio se fundamenta en tres pilares que se consideran principales.

El primero está relacionado directamente con la normativa vigente en Ecuador para el control de los ISP. Se determina que ésta se basa únicamente en la verificación del cumplimiento de parámetros de calidad del servicio final en el lado del usuario. Por la concepción y definición que poseen dichos parámetros de calidad; y considerando además el número de empresas proveedoras de Internet y el número de usuarios de cada una, se colige que el correspondiente control se fundamenta en muestreos.

Este antecedente afianza el segundo justificativo por el cual se presenta este estudio; puesto que se considera que con una adecuada gestión de riesgos (de tecnología y de la información) las empresas ISP estarían en plena capacidad de cumplir con los parámetros de calidad establecidos; además de beneficiarse de los procesos y políticas internas que dicha gestión de riesgos implementa.

Por otra parte, el tercer justificativo se encuentra intrínsecamente relacionado con la importancia del presente estudio. Como es de conocimiento, las empresas ISP

poseen como clientes a otras empresas, muchas de ellas sensibles y críticas por los servicios que prestan (financieras, gubernamentales, servicios públicos, etc.); sin embargo, dichos ISP no tienen obligación regulatoria de implementar una administración y gestión de sus riesgos de tecnología y de la información; situación que se vuelve primordial con el vertiginoso avance tecnológico que va a la par del aparecimiento de nuevas amenazas; mismas que de materializarse por la ausencia de controles, podrían no solo afectar a la empresa ISP como tal, sino involucrar a la ciudadanía en general que acude y/o es cliente de aquellas empresas "sensibles y críticas" mencionadas anteriormente.

En ese sentido, al desarrollar una metodología de la gestión de riegos, dirigida y ajustada a la realidad de los ISP de la ciudad de Quito; en su aplicación los beneficiarios directos son los mismos ISP y sus clientes (tanto residenciales como corporativos); e indirectamente beneficiaría a la ciudadanía en general (como clientes de aquellas entidades que se aprovisionan del servicio de los ISP); así como a terceras empresas como proveedores y distribuidores.

1.4. Planteamiento del problema.

Como ya se mencionó anteriormente, no se han encontrado publicaciones e investigaciones que permitan tener un panorama global respecto del nivel y madurez con el cual las empresas afrontan o están preparadas en sus procesos de administración de riesgos, específicamente de aquellas organizaciones cuyo negocio principal apunta directamente a las Tecnologías de la Información y Comunicación, y en las cuales resultan mucho más críticos los continuos cambios e implementaciones que son necesarias al momento de integrar sus actividades y procesos de negocio a los avances tecnológicos. Ese el caso puntual de aquellas empresas dedicadas a la provisión de servicios de telecomunicaciones.

En virtud de la heterogeneidad de las empresas de telecomunicaciones (tanto en infraestructura, servicios y cobertura), el presente tema de tesis busca focalizar su investigación en un grupo más específico de las TELCO, considerándose para el efecto el nicho conformado por las empresas proveedoras del servicio de Internet

(ISP); y para este caso, en el Distrito Metropolitano de Quito. De acuerdo a los datos que maneja la Superintendencia de Telecomunicaciones, a mayo de 2014 existieron cincuenta y siete (57) ISP autorizados para proveer sus servicios en esta ciudad; por lo que para el estudio propuesto se tomará una muestra compuesta por las empresas más representativas.

Es importante mencionar que en Ecuador, de acuerdo al Reglamento General a la Ley Especial de Telecomunicaciones Reformada[5], los ISP jurídicamente se reconocen como Permisionarios para la explotación de Servicios de Valor Agregado modalidad Internet; cuyo control técnico le corresponde a la Superintendencia de Telecomunicaciones. Sin embargo, la normativa en el país define para los ISP un control basado en el cumplimiento de parámetros de calidad[6] con valores objetivos que están obligados cumplir; y que, en cierto grado, buscan garantizar la calidad del servicio final en el lado del usuario.

Por lo tanto, es claro que el control a los ISP en Ecuador no está orientado hacia los procesos internos de estas empresas o a las políticas que tengan implementadas. Esta situación brinda la oportunidad para que cada organización ejecute sus propios procesos, procedimientos y metodologías que redundarían en un servicio de calidad. Obviamente, dentro de aquellos procesos se encuentran los implementados por cada ISP para la identificación, análisis, evaluación y mitigación de riegos que son responsabilidad directa de las Gerencias y Directivas.

En ese sentido, el estudio de investigación propuesto busca determinar el nivel en que los ISP en la ciudad Quito administran sus riesgos tecnológicos. Es decir, en cierto modo, tratar de determinar si las políticas de administración de riesgos tecnológicos son parte de la cultura empresarial en este sector.

---

[5] Decreto 1790 (Registro Oficial 404, 4-IX-2001); y, Decreto 2727 (Registro Oficial 599, 18-VI-2002).

[6] Resolución 216-09-CONATEL-2009 emitida por el Consejo Nacional de Telecomunicaciones el 29 de julio de 2009.

Posteriormente, sobre la base de la información obtenida, el estudio busca desarrollar una propuesta metodológica que sea adaptable a las empresas de este tipo y que coadyuve a las altas gerencias y mandos medios a identificar y evaluar los riesgos tecnológicos en una empresa proveedora de Internet en nuestro medio; y bajo ese aspecto, crear conciencia entre las empresas para que reconozcan y consideren la importancia de una adecuada administración de riesgos para la consecución de sus objetivos del negocio.

Finalmente, el propósito del estudio es determinar las bondades de la propuesta metodológica desarrollada al ensayarse sobre una empresa especifica dedicada a la provisión del servicio de Internet, la misma que se verá beneficiada de contar al final del proceso con una matriz de sus riesgos tecnológicos y de las recomendaciones que a partir de allí, el equipo evaluador pueda emitir. Luego, si bien dichas recomendaciones le pudieran servir de insumo a este ISP, su ejecución e implementación no son parte del alcance del estudio propuesto.

1.5. Formulación del problema

- ¿Cuál es el nivel de la gestión de riesgos en las empresas proveedoras de servicios de Internet en la ciudad de Quito?

- ¿En términos de TI una empresa del sector corre un alto riesgo si no se define una metodología para la gestión del riesgo informático?

- ¿En qué medida disponer de una propuesta metodológica contribuiría a la gestión de riesgos tecnológicos en una empresa proveedora de Servicios de Internet?

1.6. Hipótesis

La aplicación de la propuesta metodológica de gestión de riesgos tecnológicos permite contar con indicadores para minimizar los riesgos tecnológicos.

1.7. Objetivo General

Elaborar una propuesta metodológica de gestión del riesgo tecnológico para empresas del sector de las telecomunicaciones dedicadas a la provisión del servicio de Internet (ISP).

1.8. Objetivos Específicos

- Determinar el grado con el cual se administran los riesgos tecnológicos en el sector de las empresas proveedoras del servicio de Internet (ISP) del Distrito Metropolitano de Quito; mediante la aplicación de encuestas y entrevistas a personal clave de una muestra de dichas compañías.

- Desarrollar una propuesta metodológica de gestión de riesgos tecnológicos ajustada a las necesidades y escenarios de un ISP del medio local, en función de los resultados que arroje el estudio de investigación en el sector.

- Aplicar la propuesta metodológica de gestión de riesgos tecnológicos a una empresa particular dedicada a la provisión de servicios de Internet en la ciudad de Quito (ISP).

- Emitir recomendaciones al ISP en mención para la administración de sus riesgos tecnológicos sobre la base de la evaluación aplicada.

1.9. Operacionalización de variables

1.9.1. Variable independiente.

Según Hernández, R. Sampieri (2006) se define a la variable independiente como la supuesta causa en una relación entre variables, es la condición antecedente. En este contexto para el presente trabajo de investigación la variable independiente identificada será: La investigación respecto al nivel de madurez con el cual las empresas proveedoras del servicio de Internet (ISP) de la ciudad de Quito gestionan los riesgos tecnológicos.

1.9.2. Variable dependiente

Hernández, R. Sampieri (2006) define a la variable dependiente como al efecto provocado por la variable independiente, es la condición consecuente. Así, para el presente trabajo de investigación la variable dependiente será: El desarrollo de una propuesta metodológica para la gestión de riesgos en empresas del Servicio Valor Agregado, modalidad Internet, aplicada sobre una empresa tipo.

Tabla 1

Operacionalización de variables.

OBJETIVO	VARIABLES	DIMENSIONES	INDICADORES
Elaborar una propuesta metodológica de gestión de riesgos tecnológicos para empresas del sector de las telecomunicaciones dedicadas a la provisión del servicio de Internet (ISP) y aplicarla sobre un caso de estudio.	Nivel de madurez de gestión de riesgos tecnológicos en ISP de Quito.	Investigación	Nivel madurez de ISP en Quito respecto a gestión del riesgo.
	Propuesta metodológica para la gestión de riesgos tecnológicos	Establecimiento del contexto	Actas de aprobación y comunicación.
		Análisis de riesgos	Levantamiento de activos, amenazas y controles existentes.
		Evaluación de riesgos	Priorización de riesgos.
		Respuesta a los riesgos	Recomendaciones para evitar, reducir, compartir o aceptar riesgos.

CAPITULO II.

MARCOS DE REFERENCIA PARA LA ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS.

2.1. MAGERIT versión 3

2.1.1. Descripción general

MAGERIT- versión 3.0 es una metodología de análisis y gestión de riesgos de sistemas de información elaborada por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica del Gobierno de España, presentada en 3 libros distribuidos de la siguiente manera:

- Libro I – Método.
- Libro II – Catálogo de Elementos.
- Libro III – Guía de Técnicas.

Dicho de manera general, MAGERIT permite estudiar los riesgos que soporta un sistema de información y el entorno al que se encuentra asociado. El objetivo que esta metodología persigue, es principalmente el crear conciencia a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos; y lo hace ofreciendo un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones, además de ayudar a planificar el tratamiento oportuno para mantener los riesgos bajo control.

Así, MAGERIT propone la ejecución de un análisis de riesgos basado en evaluaciones del impacto que alcanzaría en la organización una trasgresión a las medidas de seguridad. Además de señalar los riesgos existentes, MAGERIT ayuda a identificar las amenazas a las que se encuentra expuesto el sistema de información y a determinar la vulnerabilidad de los sistemas de control y/o prevención.

Ese análisis de riesgos permite contar con resultados, como la relación de amenazas posibles, mapa de riesgos, relación de salvaguardas implementadas y

requeridas, impactos potenciales y residuales, riesgos potenciales y residuales, entre otros, base sobre los cuales es posible emitir recomendaciones adecuadas para gestionar esos riesgos.

Es decir, MAGERIT proporciona los resultados necesarios para ejecutar además una etapa de gestión de riesgos en la que se puedan recomendar medidas que deberían adoptarse para aceptar, mitigar, evitar o compartir los riesgos identificados.

Esta metodología, de acuerdo a la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica del Gobierno de España, prepara a una Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. Por su contribución es considerada como un estándar de facto.

2.1.2. Descripción específica

El Libro I – Método de MAGERIT – versión 3.0, propone dos grandes tareas a realizar: el Análisis de riesgos y la Gestión de los riesgos. Para el Análisis de riesgos, considera:

- Activos, que son los elementos del sistema de información que soportan los objetivos de negocio (misión) de la Organización.
- Amenazas, que son situaciones en las que pueden verse inmiscuidos los activos causando un perjuicio a la Organización.
- Salvaguardas o contra medidas, que son medidas de protección desplegadas para que aquellas amenazas no causen daño o reduzcan su impacto.

El Análisis de riesgos permite estudiar estos elementos de forma metódica para estimar dos factores fundamentales: el riesgo y su impacto; y posteriormente llegar a conclusiones con fundamento para proceder a la fase de gestión. Es decir, disponer de información para tomar decisiones conociendo los activos a proteger, las amenazas y las salvaguardas valoradas. A partir de aquí, la Gestión de riesgos actúa en dos pasos:

- Evaluación; y,

- Tratamiento.

La evaluación de los riesgos va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como también bajo qué circunstancias se puede aceptar un riesgo o trabajar en su tratamiento.

Por su parte, el tratamiento de los riesgos recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta dos grandes opciones:

- Reducir el riesgo residual (aceptar un menor riesgo); o,

- Ampliar el riesgo residual (aceptar un mayor riesgo)

Para tomar una u otra decisión, MAGERIT enmarca los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre:

- Cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- Posibles beneficios derivados de una actividad que en sí entraña riesgos
- Condicionantes técnicos, económicos, culturales, políticos, etc.
- Equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, etc.

Finalmente es importante recalcar que de acuerdo al Libro I – Método, la gestión de los riesgos en MAGERIT – VERSIÓN 3.0 está estructurada de forma metódica basada en la norma ISO 31000 proponiendo el esquema que se muestra a continuación:

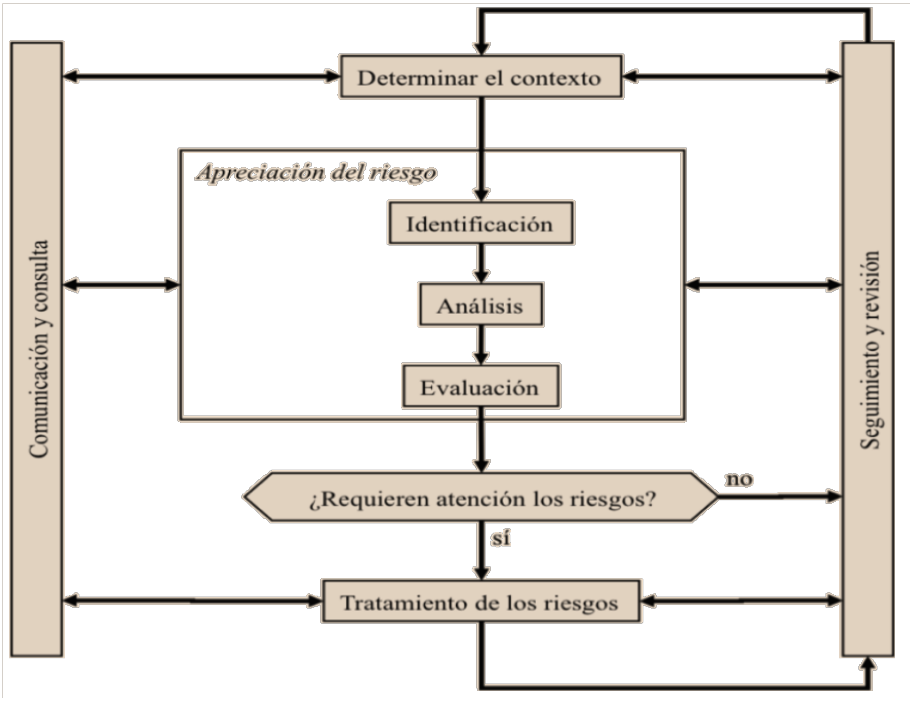


Figura 3. Esquema para gestión de Riesgos MAGERIT v3.0
Fuente: MAGERIT v3.0

Se debe observar que paralelo al Análisis y Gestión de riesgos descritos antes, MAGERIT – versión 3.0 incorpora los procesos de Comunicación y consulta; y, Seguimiento y revisión. La metodología establece que siempre se debe buscar un equilibrio entre seguridad y productividad de la Organización y que dentro de ese equilibrio resulta fundamental un proceso de comunicación con la colaboración de varios interlocutores como:

- Los usuarios, cuyas necesidades deben ser consideradas y quienes deben estar plenamente informados para que colaboren activamente en la operación del sistema dentro de los parámetros de seguridad.

- Proveedores externos, a quienes se deben proporcionar instrucciones claras para exigir el cumplimiento de los niveles de servicio requeridos así como la gestión de eventuales incidentes de seguridad.

- Órganos de gobierno que deberán establecer los canales de comunicación adecuados para consolidar la confianza de que el sistema de información está en la capacidad de responder adecuadamente para atender a la misión de la Organización.

Por otra parte, el proceso de Seguimiento y revisión que propone MAGERIT, pretende notar que el análisis de riesgos es una actividad en la que es imprescindible el monitoreo y actuar en consecuencia, reaccionando acuciosamente a los incidentes, y mejorando continuamente el conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

2.1.3. Técnicas de identificación de riesgo

El Libro III – Técnicas de MAGERIT versión 3.0 describe algunas técnicas utilizadas para el análisis y gestión de riesgos que podrían utilizarse sin ayudas o herramientas automatizadas.

La metodología establece técnicas generales que son de utilidad en el desarrollo de un proyecto de análisis y gestión de riesgos, considerando de especial interés las siguientes:

- Técnicas gráficas:
    - Histogramas (puntos, barras, radar)
    - Diagramas de Pareto, para priorización de acciones.
    - Diagramas de pastel.

- Sesiones de trabajo:
    - Entrevistas, dirigidas a obtener la información de una forma individual dónde aparecen los perfiles de entrevistado y entrevistador.

    - Reuniones, que pueden tener el mismo objetivo, pero la información está dispersa entre varias personas y únicamente trabajando en grupo, se conseguirá extraer y depurar toda la información de forma global.

    - Presentaciones, cuyo objetivo es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda.

- Valoraciones Delphi:
    - Técnica netamente cualitativa que relativamente permite tratar con alta precisión problemas técnicamente complejos; y está planteada como una reflexión organizada de expertos sobre un tema concreto, reflexión que permite recoger las ideas y opiniones más cualificadas en el ámbito de la seguridad (valoración de activos e identificación de amenazas e impactos).

Luego, MAGERIT – versión 3.0, propone el uso de las siguientes técnicas de tipo específicas para el tratamiento de los resultados obtenidos con las técnicas generales detallas antes:

- Uso de tablas para la obtención sencilla de resultados.
- Técnicas algorítmicas para la obtención de resultados elaborados.
- Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información.

2.1.4. Técnicas de evaluación de riesgo

Conforme el Libro I - Método de MAGERIT 3.0, la evaluación de riesgos corresponde a las tareas de interpretación de los resultados; es decir, de los valores de impacto y riesgos residuales. Las técnicas que pueden emplearse por lo tanto son las descritas anteriormente:

- Técnicas gráficas:
    - Histogramas, diagramas de Pareto y de pastel.
- Sesiones de trabajo:
    - Entrevistas
    - Reuniones

  - Presentaciones

- Valoraciones Delphi

2.1.5. Tratamiento de riesgos

El tratamiento de los riesgos identificados y calificados se plasman en el Plan de Seguridad de la Información, su elaboración se apoya en las siguientes técnicas:

- Análisis Costo - Beneficio
- Planificación de proyectos

Es importante destacar que MAGERIT considera que la única forma de afrontar la complejidad propia de un proyecto de análisis y gestión de riesgos es centrarse en lo más importante, es decir, se debe comenzar a tratar los riesgos que resulten con máximo impacto y máximo riesgo.

2.2. Norma ISO/IEC 27005: 2012

2.2.1. Descripción general

La norma ISO/IEC 27005, es elaborada por el subcomité SC 27 Técnicas de Seguridad que forma parte del comité técnico ISO/IEC JTC 1 Tecnologías de Información, establecido conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrónica Internacional (IEC).

En Ecuador, el Instituto Ecuatoriano de Normalización INEN ha adoptado como norma la ISO/IEC 27005:2012, y expidió la denominada NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27005:2012. Ésta contiene recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la Información, es compatible con los conceptos generales especificados en la norma

ISO/IEC 27001 y está diseñada como soporte para aplicar satisfactoriamente en un SGSI[7] basado en un enfoque de gestión de riesgos.

El riesgo se define como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daños. El riesgo de Tecnología de Información (TI) está relacionado con el uso, propiedad, operación, distribución y la adopción de las tecnologías de la Información en una organización.

Aunque la norma no propone un método concreto de cómo gestionar riesgos, recomienda usar un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de tratamiento de riesgos.

En general, los indicadores de riesgo de la norma ISO/IEC 27005 (NTE INEN-ISO/IEC 27005:2012) muestran si la organización tiene una alta probabilidad de ser expuesta a un riesgo que excede el impacto permitido.

2.2.2. Descripción específica

A continuación se lista los procesos y actividades que conceptualmente contempla la norma ISO/IEC 27005: 2012.

- **Proceso 1: Establecimiento del Contexto**

    - Definición de criterios básicos
        - De evaluación del riesgo
        - De Impacto
        - De la aceptación del riesgo
    - Alcance y límites
    - Organización para la gestión del riesgo de la seguridad de la información

[7] SGSI, Sistema de Gestión de Seguridad de la Información.

- **Proceso 2: Valoración del Riesgo**
  - Análisis del riesgo
    - Identificación del riesgo
      - Identificación de activos
      - Identificación de amenazas
      - Identificación de controles existentes
      - Identificación de vulnerabilidades
      - Identificación de consecuencias
    - Estimación del riesgo
      - Metodologías para estimar el riesgo
      - Valoración de las consecuencias
      - Valoración de los incidentes
      - Nivel de estimación del riesgo
  - Evaluación del riesgo

- **Proceso 3: Tratamiento del Riesgo**
  - Reducción del riesgo
  - Retención del riesgo
  - Evitación del riesgo
  - Transferencia del riesgo

- **Proceso 4: Aceptación del Riesgo**

- **Proceso 5: Comunicación de los Riesgos**

- **Proceso 6: Monitoreo y Revisión del Riesgo**
  - Monitoreo y revisión de los factores del riesgo
  - Monitoreo, revisión y mejora de la gestión de riesgos

Estos procesos se resumen en la gráfica del Proceso de Gestión de Riesgos de la Seguridad de la Información incluida en la norma NTE INEN-ISO/IEC 27005:2012:

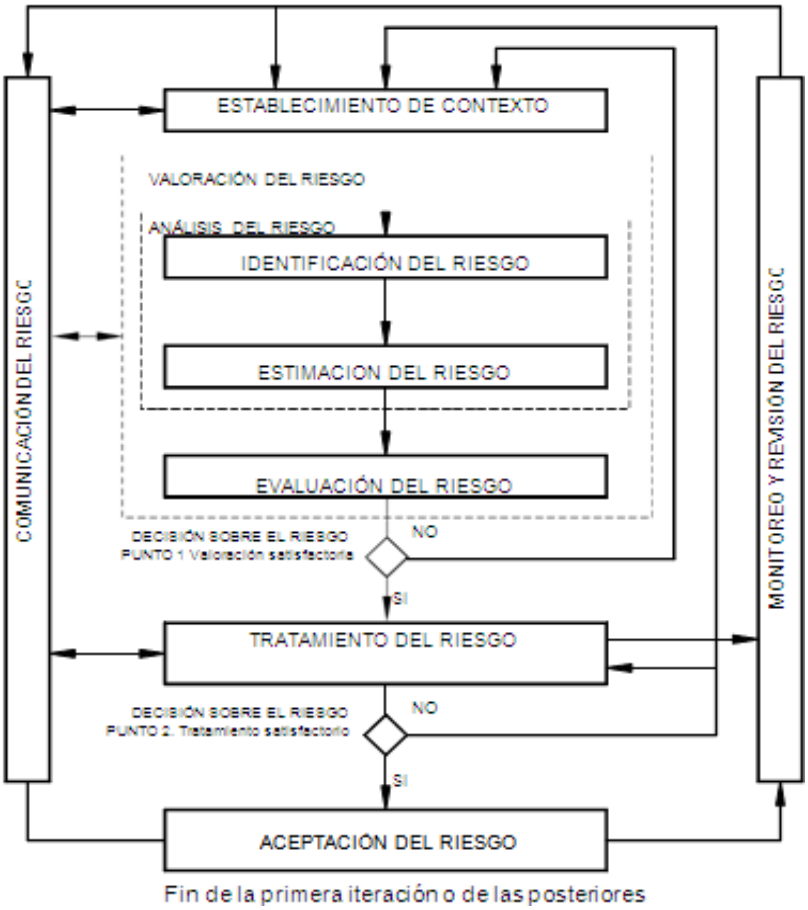


Figura 4. Norma Técnica Ecuatoriana NTE INEN-ISO/IEC27005:2012
Fuente: Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27005:2012

2.2.3. Técnicas de identificación de riesgos

Como se mencionó antes, la identificación del riesgo pertenece al Proceso 2: Análisis del Riesgo de la norma ISO/IEC 27005:2012.

Esta norma no provee técnicas específicas para la identificación de riesgos; sin embargo, su guía de implementación menciona la valoración de la información a través de entrevistas a personas de la gerencia de la Organización.

Es decir, recopilar información de aquellas personas que pueden hablar con autoridad acerca de la determinación del valor y la sensibilidad de la información en términos de los escenarios más desfavorables cuya ocurrencia se esperaría a partir de consecuencias adversas para el negocio.

2.2.4. Evaluación de riesgos

La evaluación de riesgos se ejecuta en puntos discretos de tiempo proporcionando una visión temporal de los riesgos evaluados. Se realiza a menudo en más de una iteración. La primera es una evaluación de alto nivel para identificar los riesgos altos, mientras que las iteraciones posteriores determinan los riesgos principales y tolerables.

El propósito de una evaluación del riesgo es determinar si las contramedidas o salvaguardas son adecuadas para reducir la probabilidad de la pérdida o para que el impacto de esa pérdida alcance un nivel aceptable.

La norma ISO/IEC 27005: 2012 no detalla ni profundiza respecto de las técnicas que deben aplicarse para llevar a cabo una evaluación de riesgos. Únicamente precisa que dichas metodologías pueden variar desde los enfoques cualitativos o cuantitativos a cualquier combinación de ellos. Adicionalmente, brinda la posibilidad de escoger métodos basados en tablas y combinaciones de medidas subjetivas y empíricas.

Señala que lo principal es que la Organización se sienta cómoda con el método empleado y que proporcione resultados que sean confiables. Por otra parte, para la evaluación del riesgo, la norma brinda una guía de implementación, en la que pueden utilizarse técnicas basadas en tablas (Anexo E de la norma); por ejemplo, una matriz de valoración de riesgos en la que los activos de la organización se evalúan en términos de costo de reemplazo o de reconstrucción. En todo caso, la norma ISO/IEC 27005: 2012 indica que para la evaluación de riesgos se requerirá de la ejecución de estudios de:

- Vulnerabilidades, amenazas, probabilidad, pérdidas o impacto.
- Eficiencia de las medidas de seguridad; e,
- Identificación de los activos.

Y adicionalmente establece la implementación de funciones de protección (controles) previo a la realización de:

- Análisis costo/beneficio de la salvaguarda; y,
- Análisis de la sensibilidad/valor de los bienes que se protegen.

2.2.5. Tratamiento de riesgos

El propósito de definir una respuesta al riesgo es llevar el riesgo a un nivel tolerable. Es decir, el riesgo residual debe estar dentro de los límites de tolerancia al riesgo. El riesgo en ISO/IEC 27005: 2012 puede ser manejado de acuerdo a cuatro estrategias principales (o una combinación de ellas):

- Evitar el riesgo, aislando las actividades que dan lugar al riesgo.
- Mitigar el riesgo adoptando medidas que detectan y reducen el impacto del riesgo.
- Transferir riesgos a otras áreas menos susceptibles o a otras entidades con más experiencia (outsourcing).
- Aceptar riesgos que se corren deliberadamente y que no se pueden evitar, sin embargo es necesario identificarlos, documentarlos y medirlos.

2.3. Marco de referencia COBIT

2.3.1. Descripción general

Publicado por ISACA, una asociación internacional dedicada a proveer el conocimiento tecnológico tanto en gobierno, control, seguridad, riesgo y auditoría de información, es encargada en presentar continuamente las actualizaciones del marco referencial COBIT a nivel mundial, con el propósito de encaminar a los profesionales en la gestión y gobierno de TI.

COBIT, es una metodología que se ha convertido en una de las más aceptadas y utilizadas a nivel mundial ya que se presenta como un marco de referencia general de gobierno de TI y permite el desarrollo de las mejores prácticas en cada una de las

aéreas de una organización, ayudando a comprender y administrar los riesgos siempre orientado al negocio otorgando a los líderes o gerentes una visión completa de TI al momento de la toma de decisiones.

COBIT 5 es la última versión publicada por ISACA, este marco de trabajo se enfoca al Gobierno Corporativo de TI y en uno de sus principios manifiesta la necesidad de separar el gobierno de la administración. En esta versión se presenta un nuevo dominio EDM (Evaluar, Dirigir y Monitorear), específicamente para gobierno y el total de procesos aumenta a 37.

2.3.2. Descripción específica

COBIT es un marco para el gobierno y la gestión de las tecnologías de información que permite a la gerencia conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio.

El Gobierno asegura el logro de los objetivos de la Organización, al evaluar las necesidades de las partes interesadas, así como las condiciones y opciones; fijando directivas al establecer prioridades y tomar decisiones; así como monitorear el desempeño, cumplimiento y progreso, comparándolos contra las directivas y objetivos acordados.

La Administración planifica, construye, ejecuta y monitorea las actividades conforme a las directivas fijadas por el ente de Gobierno para lograr los objetivos de la Organización. Los 5 principios para la construcción de un marco de gobierno de TI, se detallan como:

1. Satisfacer las necesidades de los interesados.
2. Cubrir la empresa de extremo a extremo.
3. Aplicar un solo marco integrado.
4. Habilitar un enfoque Holístico.
5. Separar Gobierno de Administración.

La gestión se basa en un conjunto holístico de **siete facilitadores** que optimizan la información, la inversión en tecnología y el uso para el beneficio de las partes interesadas, estos son:

1. Principios, políticas y marcos de trabajo.
2. Procesos.
3. Estructura organizacional.
4. Cultura, ética y conducta.
5. Información.
6. Servicios, infraestructura y aplicaciones.
7. Personas, habilidades y competencias.

La administración de Riesgos.- Es inevitable pasar por desapercibido los riesgos de tipo tecnológico, la tendencia a crecer por parte de las empresas los llevan a implementar grandes cambios como adquirir nueva aplicación, equipo o recurso de TI, esto puede traer consigo nuevos riesgos que deben ser identificados, administrados y monitoreados para prevenir la ocurrencia de eventos que podrían tener un impacto negativo en los objetivos de negocio.

COBIT 5 en el dominio de Gobierno, presenta el proceso **EDM03** denominado Asegurar la optimización de riesgos.

- La descripción de este proceso según COBIT es la siguiente:
  Asegurar que el apetito de riesgo de la empresa y la tolerancia se entiende, es articulado y comunicado, y que el riesgo de valor de la empresa en relación con el uso de las TI es identificado y gestionado.

- Proceso de declaración de propósito por COBIT
  Asegurar que los riesgos relacionados con TI de la empresa no superen la tolerancia al riesgo y el apetito de riesgo, que el impacto de los riesgos de TI de valor de la empresa es identificado y manejado, y que la posibilidad de fallas de cumplimiento es mínima.

Otro dominio de Gestión sobre riesgos es Alinear, Planear y Organizar, este contiene un proceso de riesgos relacionados **APO12** denominado Gestionar el riesgo.

- Descripción del proceso por COBIT.
  Continuamente identificar, evaluar y reducir los riesgos relacionados con TI dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

- Proceso de Declaración de Propósito por COBIT.
  Integrar la gestión de riesgos empresariales (ERM) relacionados con la TI con el ERM en general, y equilibrar los costos y beneficios de la gestión de riesgos relacionados con TI de la empresa.

2.3.3. Técnicas de identificación y evaluación de riesgos

COBIT como marco de referencia permite crear un enfoque de riesgos, que parte con el análisis de la situación actual para identificar los procesos y activos de tecnología de la organización a evaluar y así definir la criticidad que tiene cada uno, para posteriormente identificar el tipo y nivel de riesgos al que se encuentran sometidos.

COBIT 5 ha integrado el contenido de COBIT 4.1, Val IT and Risk IT en un Modelo de Referencia de Procesos. Éste último se basa en los siguientes componentes: Gobierno del Riesgo, Evaluación del Riesgo y Respuesta al Riesgo. Algunas técnicas que ayudan al levantamiento de información son:

- Reuniones necesarias
- Solicitudes de autorización o aprobación a cierta información.
- Observación,
- Entrevistas y encuestas.
- Cuestionarios

El enfoque de riesgos permite tener una visión categorizada basada en COBIT de los diferentes riesgos a los que se encuentra sometida la organización lo que permitirá obtener la probabilidad e impacto de ocurrencia utilizando diferentes técnicas de evaluación como las siguientes:

- Clasificación o categorización de riesgos.
- Escalas de estimación: Permite dar prioridad a los riesgos, por ejemplo la escala puede estar definida como Alto, medio, bajo.
- Matriz de riesgos, (alto, medio, bajo)
- Fórmulas matemáticas: servirán para asignar una calificación al riesgo.

2.3.4. Tratamiento de los riesgos

Se considera los siguientes aspectos para enfrentar los riesgos identificados según la evaluación efectuada.

1. Evitar el riesgo
2. Reducción/mitigación del riesgo
3. Compartir/Transferir el riesgo
4. Aceptar el riesgo

Con el apoyo de alta gerencia se podrán efectuar planes o planificación de proyectos considerando siempre el costo/beneficio.

2.4. GTAG (Guías de Auditoría de Tecnología Global)

2.4.1. Descripción general

Las guías de auditoría global, preparadas por el IIA (Instituto de Auditores Internos), han sido elaboradas con un lenguaje y pautas muy claras que permiten enfrentar los problemas e inconvenientes de muchos cambios y avances relacionados con la tecnología de la información, el riesgo, el control y la seguridad.

Cada guía sirve como un recurso para los auditores y también para personal involucrado con las TI dentro de la organización. Una de las pautas que ofrecen estas guías son las relaciones entre los riesgos del negocio, los controles clave dentro de los procesos de negocio, controles automáticos y otras funciones críticas de TI.

2.4.2. Descripción específica

La **Guía N° 6** denominada Gestión y auditoria de puntos vulnerables de tecnología de la información), manifiesta que en la seguridad de la información, así como la gestión de tecnología de la información, es de gran responsabilidad asegurar que los riesgos tecnológicos se gestionan adecuadamente, riesgos que se originan en el despliegue y el uso de los activos de TI.

El ciclo de vida de la gestión de vulnerabilidades es uno de los puntos principales de esta guía, en la cual se trata la evaluación de riesgos y el establecimiento de sus prioridades. Todo riesgo puede ser identificado y aplicar una solución evaluando su probabilidad e impacto. El ciclo de vida es el siguiente:

- Identificación y validación.
- Evaluación de riesgos
- Procesos de mitigación
- Mejora continua.

La organización debe tener un proceso bien definido para medir los riesgos que pueda ser aplicado de manera precisa, se considera también el hecho de que pueden existir riesgos aceptados debido a su baja probabilidad e impacto. Las prioridades también son establecidas en función de la criticidad del activo.

1. Identificación y validación.

1.1 Sistemas de determinación de alcance.

Obtener una lista completa de todos los segmentos de red utilizados a través de la organización, por ejemplo redes corporativas cableadas e

inalámbricas, se debe identificar y documentar cada una de estas redes. Se debe incluir una arquitectura de red que muestre las interconexiones y los dispositivos. La identificación ayuda a obtener un inventario de la red y todos los activos de tecnología dentro de la organización

1.2 Detectar vulnerabilidades.

Es fundamental realizar una escaneo o supervisión periódica para detectar posibles vulnerabilidades que pueden presentarse en cada uno de los activos de tecnología.

Existen aplicaciones especiales que examinan los diferentes activos de TI para identificar debilidades y son programados para ejecutarse con diferentes frecuencias, sean diarias, mensuales, según las necesidades.

1.3 Validar los hallazgos.

La organización validará los resultados obtenidos después del escaneo o supervisión. Cabe recalcar que pueden existir errores “falsos positivos” o “falsos negativos”.

2. Evaluación de riesgo.

2.1 Evaluar el riesgo.

Con las vulnerabilidades adquiridas se determina el riesgo real que representa dentro de la organización, se debe disponer de un procedimiento bien definido para medir los riesgos que sea aplicable de manera rápida y precisa.

Un punto vulnerable en muchos casos no es tratado debido a que la organización puede optar por aceptar el riesgo según su probabilidad e impacto que cause dentro de la misma.

2.2. Establecer prioridades entre las vulnerabilidades

Establecer las prioridades de las vulnerabilidades de acuerdo a la criticidad del activo tomando en cuenta la probabilidad y frecuencia con la que pueda ocurrir un ataque. Muchas de las veces se compara el riesgo real con el costo de implementación de la corrección al punto vulnerable y se establece su prioridad en función de su eficacia con relación al costo.

3. Mitigar las vulnerabilidades.

3.1 Mitigar las vulnerabilidades críticas.

Disponer de procedimientos operativos que aseguren que el personal apropiado de seguridad de TI aborde la implementación de correcciones de manera oportuna. Esto procedimientos pueden estar basados en incidentes anteriores.

3.2. Crear un proceso para mitigar las vulnerabilidades.

El propósito es disponer o elaborar un proceso para mitigar las vulnerabilidades más críticas, establecer planes y al personal adecuado para ejecutarlos. Hay que recalcar que al riesgo no se lo puede eliminar pero si mitigarlo, disminuyendo la probabilidad de que ocurra. La manera más eficiente de enfrentar este problema es con la creación de un proyecto de TI en el que incluya un gerente, entrega de procesos y fecha límite. Este proyecto debe tener la autoridad para integrarse con otros procesos necesarios en la ejecución del mismo.

4. Mejora continua.

4.1. Detener la propagación.

La seguridad de TI debe notificar a Gestión de cambio sobre cualquier modificación de sistemas o aplicaciones.

4.2 Fijar las expectativas en función de los acuerdos de nivel de operaciones.

4.3 Usar las experiencias pasadas para guiar las acciones futuras, la organización puede utilizar los indicadores necesarios tanto los basados en experiencias de fracaso y los de éxito.

2.4.3. Técnicas de identificación.

Las guías de auditoría de tecnología global presentan recursos para la recopilación de información dentro de una organización, tanto para identificación de activos procesos y vulnerabilidades. Algunas técnicas para la recopilación de datos según la GTAG 6 tenemos.

- Métricas de gestión de puntos vulnerables.

- Las 10 preguntas principales del auditor sobre gestión de puntos vulnerables.

2.4.4. Técnicas de evaluación de riesgos

En la GTAG 11 (Desarrollo de la Auditoría de TI) se encuentran técnicas de evaluación. Esta guía se centra exclusivamente en las matrices ponderadas para medir riesgo e impacto. Por ejemplo para calcular la probabilidad de ocurrencia se basa en la siguiente escala:

Tabla 2
Probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA		
H	3	Alta probabilidad de ocurrencia del riesgo.
M	2	Media probabilidad de ocurrencia del riesgo.
L	1	Baja probabilidad de ocurrencia del riesgo.

Fuente: Guía GTAG-11. Developing the IT Audit Plan

De la misma forma establece una escala modelo de impacto de riesgo.

Tabla 3

Escala modelo de impacto.

ESCALA DE IMPACTO		
H	3	El potencial de impacto material es alto.
M	2	El potencial de impacto material es significativo / moderado.
L	1	El potencial de impacto material es de bajo alcance.

Fuente: Guía GTAG-11. Developing the IT Audit Plan

Dentro de estas técnicas se puede usar otras metodologías que ayuden a dar una mejor visión sobre el escenario de evaluación y procesos de auditoría.

2.4.5. Tratamiento de los riesgos

Se puede optar por aceptar ciertos riesgos o buscar mitigarlos según los resultados obtenidos. A continuación se recalcan los siguientes factores que resultan necesarios según las GTAG.

- Personal capacitado de seguridad de TI.
- Procedimientos operativos.
- Proyectos de TI.
- Apoyo de la alta gerencia.

El éxito de un proyecto eficaz para mitigar riesgos radica en el apoyo que reciba y el personal que conforme el equipo para llevar a cabo los procesos de seguridad.

CAPÍTULO III

CULTURA DE ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS EN ISP DEL DISTRITO METROPOLITANO DE QUITO.

Como se ha expresado anteriormente, la administración de riesgos tecnológicos es un proceso compuesto de trabajos, estrategias y actividades destinadas a promover acciones de mitigación y prevención ante posibles incidentes de índole tecnológico.

En las empresas proveedoras de servicios de telecomunicaciones, cuyo núcleo de negocio está relacionado directamente con las tecnologías de información y comunicación, se podría pensar a primera instancia que las mismas cuentan con procesos de gestión de riesgos tecnológicos robustos que les permitan alcanzar cumplimientos regulatorios y/o de continuidad de servicios y en los cuales se soporten adecuadamente sus objetivos de negocio.

Es así que, con el objetivo de determinar si el core del negocio de una empresa de telecomunicaciones va de la mano con sus procesos adoptados para gestionar los riesgos tecnológicos, se consideró importante y fundamental determinar cuan difundidos e implementados se encuentran los conceptos de administración de riesgos a través de la definición de un nivel de madurez; específicamente en aquellas empresas dedicadas a la provisión de Servicios de Internet; bajo el antecedente de no haberse registrado ningún estudio previo similar que perfilara el nivel con el que los ISP del Distrito Metropolitano de Quito se encuentran preparados en cuanto a la administración de sus riesgos tecnológicos.

3.1. Nivel de madurez

Existen algunos indicadores y metodologías que permiten indagar acerca del nivel de madurez en tecnologías de información en una organización, en el presente caso se requiere determinar la madurez en la gestión de riesgos tecnológicos que mantienen las empresas ISP del Distrito Metropolitano de Quito.

Una de estas metodologías en la estimación del nivel de madurez de TI es COBIT, este marco proporciona métricas y modelos de madurez en los procesos a fin de poder medir el logro de los diferentes objetivos, así como identificar los responsables de dichos procesos de negocio y los correspondientes de TI.

La evaluación de la capacidad de los procesos basada en los “modelos de madurez” de COBIT, es una parte fundamental en la implantación del gobierno de las TI. COBIT presenta una escala de 0 a 5 en su modelo de madurez para el tratamiento de la gestión de riesgos de TI, la misma que detalla lo siguiente:

- Madurez Nivel 0.- No existe ningún proceso de evaluación del riesgo TI.

- Madurez Nivel 1.- Los riesgos TI se consideran de una forma “ad hoc”. A veces se hace evaluación de los riesgos.

- Madurez Nivel 2.- Repetible pero intuitiva. Solo en proyectos importantes o cuando se detectan problemas.

- Madurez Nivel 3.- Proceso Definido y documentado. Existe un procedimiento documentado que establece cuando y como se debe realizar la evaluación del riesgo TI.

- Madurez Nivel 4.- Medido y Gestionado. No sólo existen procedimientos de identificación y gestión del riesgo, si no que se efectúan medidas y se controlan resultados.

- Madurez Nivel 5.- Optimización.

A partir de los modelos existentes como COBIT podemos adoptar una escala similar para medir la madurez en Gestión de riesgos de las empresas:

Tabla 4

Escala de Nivel de Madurez

NIVEL	DEFINICIÓN
0	No dispone.
1	No se piensa en ello de manera esencial.
2	Ocasional y/o solo en ciertos proyectos.
3	Procedimientos definidos y documentados.
4	Medido y gestionado.
5	Optimizado.

Para el efecto, se procedió a aplicar un modelo de encuesta dirigido a funcionarios encargados de la seguridad tecnológica (información y comunicaciones) en las empresas ISP que operan en el Distrito Metropolitano de Quito.

Por otra parte, según datos de la Superintendencia de Telecomunicaciones SUPERTEL, al mes de mayo del 2014, existieron registradas cincuenta y siete (57) empresas legalmente autorizadas para proveer Servicios de Valor Agregado modalidad Internet (ISP) en Quito. El listado de las mismas se muestra a continuación:

Tabla 5

Empresas ISP de la ciudad de Quito.

No.	EMPRESA (ISP)
1	CORPORACIÓN NACIONAL DE TELECOMUNICACIONES
2	SURAMERICANA DE TELECOMUNICACIONES S.A. SURATEL
3	ECUADOR TELECOM S.A.
4	MEGADATOS S.A.
5	PUNTO NET S.A.
6	SERVICIOS DE TELECOMUNICACIONES SETEL S.A.

Continúa →

7	PANCHONET S.A.
8	TRANSTELCO S.A.
9	TELCONET S.A.
10	UNIVISA S.A.
11	BRIDGETELECOM S.A.
12	LEVEL 3 ECUADOR LVLT S.A. (GLOBAL CROSSING)
13	ZENIX S.A. SERVICIOS DE TELECOMUNICACIONES SATELITAL
14	STEALTH TELECOM DEL ECUADOR
15	CONSORCIO ECUATORIANO DE TELECOMUNICACIONES S.A. CONECEL
16	OTECEL S.A.
17	NEW ACCESS S.A.
18	MILLTEC S.A.
19	TELYDATA TELECOMUNICACIONES Y DATOS
20	COMPAÑÍA BRIGHTCELL S.A.
21	TELECOMUNICACIONES NETWORKING TELYNETWORKING C.A.
22	ECUAONLINE S.A.
23	COMPUATEL MANTENIMIENTO INSTALACIONES Y ASESORIA EN TELECOMUNICACIONES CIA. LTDA.
24	GRUPO BRAVCO CIA. LTDA.
25	GRUPO MICROSISTEMAS JOVICHSA S.A.
26	EASYNET S.A.
27	ALFASAT COMUNICACIONES ClA. LTDA.
28	READYNET CIA. LTDA.
29	CORPORACIÓN POWERFAST (EX GPF CORPORACIÓN CIA. LTDA.)
30	INTERTEL CIA. LTDA.
31	ENTREPRENEURINC S.A.
32	SALAS TORRES CARLOS FERNANDO
33	SOCIEDAD INTERNACIONAL DE TELECOMUNICACIONES AERONÁUTICAS SITA
34	FLATEL COMUNICACIONES CIA. LTDA.
35	NEGOCIOS Y TELEFONÍA (NEDETEL) S.A.
36	VIRACOCHA TOCTAGUANO SEGUNDO NESTOR
37	PARTES Y ACCESORIOS DE DESARROLLO EN NEOCOMUNICACION ELECTRÓNICA , PARADYNE S.A.

Continúa →

38	BARRIONUEVO COX HARLEY DAVIDSON
39	GAVILANES PARREÑO IRENE DEL ROCIO
40	AT & T GLOBAL NEIWORK SERVICES ECUADOR CIA. L TDA.
41	SOLUVIGOTEL S.A.
42	AULESTIA BAEZ MARTHA PATRICIA
43	BRAINSERVICES S.A.
44	CABLEUNION S.A.
45	EQUYSUM EQUIPOS Y SUMINISTROS CIA. LTDA.
46	ETAPA EP.
47	LK TRO-KOM S.A.
48	CUEVA YOLANDA AZUCENA
49	GEONEWSERVICE CIA. LTDA.
50	MACIAS ZAMBRANO FERNANDO JAVIER
51	MEGAENLACE TELECOMUNICACIONES S.A.
52	COMPAÑÍA NACIONAL DEL ECUADOR CELEC EP
53	INTEGRAL DATA SERVICIOS DE TRANSMISIÓN INFORMÁTICA S.A.
54	SERVICIOS AGREGADOS Y DE TELECOMUNICACIONES NETWORK SATNET S.A.
55	PEROBELI S.A.
56	SYSTELECOM
57	TELEHOLDING S.A.

Fuente: Superintendencia de Telecomunicaciones

El modelo de encuesta aplicado se adjunta en el Anexo 1; y como se observa, está orientado a indagar en cinco aspectos que The Ernst & Young Business Risk Report (2010) en su publicación “The top 10 risks for global business”, también considera representativos:

- Políticas y prácticas de gerencia de riesgos.
- Comunicación.
- Amenazas y riesgos.
- Herramienta y tecnología; y,
- Gobierno y control.

3.2. Resultados encuestas.

Al respecto se debe indicar que conociendo todas las empresas ISP autorizadas para proveer servicios en la ciudad de Quito (datos SUPERTEL), se procedió a contactar al personal técnico de cada una con la encuesta en mención. Es decir, se contactaron a las cincuenta y siete (57) empresas ISP de Quito, recibiendo la respuesta de trece (13) de ellas:

- CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT E.P.
- SURATEL S.A.
- MEGADATOS S.A.
- PUNTONET S.A.
- TRANSTELCO S.A.
- TELCONET S.A.
- PANCHONET S.A.
- ECUADORTELECOM S.A.
- STEALTH TELECOM S.A.
- BRIDGETELECOM S.A.
- COMPUATEL S.A.
- FIXGROUP S.A.
- POWERFAST S.A.

Es importante observar que las respuestas de las empresas comercialmente más representativas están por lo tanto incluidas en el estudio de investigación. A continuación se detallan los resultados más representativos de la encuesta aplicada:

3.2.1. Respecto a políticas y prácticas de gerencia de riesgos.

El estudio investigativo refleja principalmente que:

- El 84.62% de los ISP encuestados manifestaron no poseer una política formal, implementada a la fecha, para la administración de riesgos tecnológicos.
- El 46.15% de los ISP encuestados indicaron no tener implementado ningún proceso de administración de riesgos en sus empresas; y no tenerlo previsto.

- El 61.54% de los ISP indicó no tener ninguna iniciativa en firme para implementar algún marco de referencia (Ej., COBIT, ISO27005, MAGERIT, etc.).

3.2.2. Comunicación.

- De las empresas que indicaron tener implantada una política de administración de riesgos, el 42.86% considera que ésta no se comunica satisfactoriamente a los accionistas e inversionistas.
- De las empresas encuestadas que manifestaron contar con una Política de Seguridad de la Información, el 57.14% indicó que no existe difusión satisfactoria de dicha política al personal en general.

3.2.3. Amenazas y riesgos.

- El 69.23% de las empresas encuestadas manifiestan percibir un incremento en los niveles de riesgo dadas las tendencias actuales hacia el uso de redes sociales, cómputo en nube y dispositivos personales móviles en las organizaciones.
- El 92.31% de las empresas encuestadas manifestaron no poseer a la fecha un programa de administración de riesgos de TI que maneje riesgos derivados del uso de redes sociales, cómputo en nube y dispositivos móviles.

3.2.4. Herramienta y Tecnología.

- De las empresas que manifestaron poseer un proceso de administración de riesgos (sección 3.1.1), el 85.71% indicó no usar ninguna tecnología para soportar dicho proceso a la fecha.
- El 69.23% de las empresas encuestadas manifestaron usar tecnologías de virtualización.
- El 46.15% de las empresas encuestadas no cuentan, a la fecha, con un software o control específico de administración de accesos e identidades que mitigue los riesgos asociados con los derechos de acceso a sus datos y sistemas.

3.2.5. Gobierno y Control.

- El 61,54% de los ISP encuestados indican no tener implementado a la fecha actual, un sistema de gestión de seguridad de la información.
- El 69.23 % de las empresas encuestadas manifestaron no contar con un comité de seguridad de la información.
- El 61,54% de las empresas encuestadas no tiene actualmente implementado ningún plan de respuesta a incidentes.
- El 53,85% de los ISP contactados, hasta la fecha, no han ejecutado una evaluación de riesgos tecnológicos; aunque el 15,38% de ellos lo tendría planificado.
- El 69.23% de las empresas encuestadas indican no haber contratado ninguna póliza de seguros que incluya lo relacionado con delitos informáticos.

El detalle de los resultados destacados en este apartado se presenta en el Anexo 2 del presente estudio.

3.3. Generación del modelo de madurez

En base a los resultados de las encuestas efectuadas se obtienen los siguientes valores del nivel de madurez, agrupados en los cinco dominios evaluados y que se mencionaron anteriormente:

- Políticas y prácticas de gerencia de riesgos.
- Comunicación.
- Amenazas y riesgos.
- Herramienta y tecnología; y,
- Gobierno y control.

Tabla 6

Dominio 1. Políticas y Prácticas de gerencia de riesgos.

DOMINIO 1. **Políticas y prácticas de gerencia de riesgos**	**Nivel de madurez (/5)**	**Promedio (/5)**
1.1. ¿Su empresa cuenta con una política general de administración de riesgos tecnológicos y ha sido comunicada internamente?	1,08	1.81
1.2. ¿Su empresa tiene un mapa de riesgos (identificación, descripción y priorización)	1,08	
1.3. ¿Su empresa tiene implantado un proceso de administración de riesgos?	1,38	
1.4. ¿Esta implementado alguno de los marcos de referencia como COBIT, COSO, ISO, MAGERIT u OTRO?	0,69	
1.5. ¿Existe alguna actividad de auditoría informática en su empresa?	0,54	
1.6. De haberla y en su opinión ¿qué tipo de relación existe entre la administración de riesgos y la función de auditoría?	4,50	
1.7. En su opinión, ¿Hasta qué punto está involucrada la administración de riesgos en el trabajo de control interno realizado para cumplir con los requerimientos regulatorios?	3,43	

Tabla 7

Dominio 2. Comunicación.

DOMINIO 2. Comunicación	**Nivel de madurez (/5)**	**Promedio (/5)**
2.1. En su opinión, ¿su empresa comunica a sus accionistas e inversionistas sus políticas y acciones de administración de riesgos?	1,43	2,08
2.2. ¿Hasta qué punto su empresa revela sus riesgos en el reporte de información (reporte anual, documentos de referencia, etc.)?	2,86	
2.3. ¿Hasta qué punto su empresa revela sus programas de seguros en su reporte de información financiera?	2,33	
2.4. ¿Existe una Política de Seguridad de la Información?	1,85	
2.5. De existir y en su opinión, ¿su empresa difunde las políticas de seguridad de la Información satisfactoriamente al personal en general?	1,43	
2.6. En su opinión, ¿el personal conoce las consecuencias que se pudieran derivar y las responsabilidades en que pudieran incurrir en caso de incumplimiento de la normativa de seguridad?	2,57	

Tabla 8

Dominio 3. Amenazas y Riesgos.

DOMINIO 3. Amenazas y riesgos	**Nivel de madurez (/5)**	**Promedio (/5)**
3.1 Considerando el ambiente económico actual, ¿ha percibido cambios en las amenazas que enfrenta su organización?	1,69	1.23
3.2 Dadas las tendencias actuales hacia el uso de redes sociales, cómputo en nube y dispositivos personales móviles en las organizaciones, ¿percibe cambios en el ambiente de riesgos que enfrenta su organización?	1,23	
3.3 ¿Cuenta con un programa de administración de riesgos de TI establecido que maneje estos riesgos derivados del uso de redes sociales, cómputo en nube y dispositivos personales móviles?	0,77	

Tabla 9

Dominio 4. Herramienta y tecnología.

DOMINIO 4. Herramienta y Tecnología	**Nivel de madurez (/5)**	**Promedio (/5)**
4.1 ¿Su organización usa alguna tecnología específica para soportar el proceso de administración de riesgos?	0,71	2,06
4.2 Su organización usa actualmente tecnologías de virtualización?	3,23	
4.3 ¿Su organización cuenta con un software o control específico de administración de accesos e identidades que mitigue los riesgos asociados con los derechos de acceso a sus datos y sistemas?	2,23	

Tabla 10

Dominio 5. Gobierno / Control.

DOMINIO 5. Gobierno / Control	Nivel de madurez (/5)	Promedio (/5)
5.1 ¿Su organización ha implementado un sistema de gestión de seguridad de la información que contemple la administración general de ésta?	2,00	1,96
5.2 ¿Su organización cuenta con un comité de seguridad de la información (CSI)?	1,23	
5.3 ¿Su organización posee un plan de respuesta a incidentes de seguridad?	1,85	
5.4. ¿Se ha realizado una evaluación de riesgos tecnológicos?	1,92	
5.5. ¿Se ha contratado una póliza de delitos informáticos?	2,08	
5.6. ¿Tienen planes de contingencia y/o continuidad de negocio?	2,69	

Tabla 11

Consolidación de resultados.

No.	DOMINIO	Promedio (/5)
1	Políticas y prácticas de gerencia de riesgos	**1,81**
2	Comunicación	**2,08**
3	Amenazas y riesgos	**1,23**
4	Herramienta y tecnología	**2,06**
5	Gobierno / control	**1,96**

Los resultados se muestran en un diagrama de radar en donde cada dominio corresponde a un eje de evaluación:

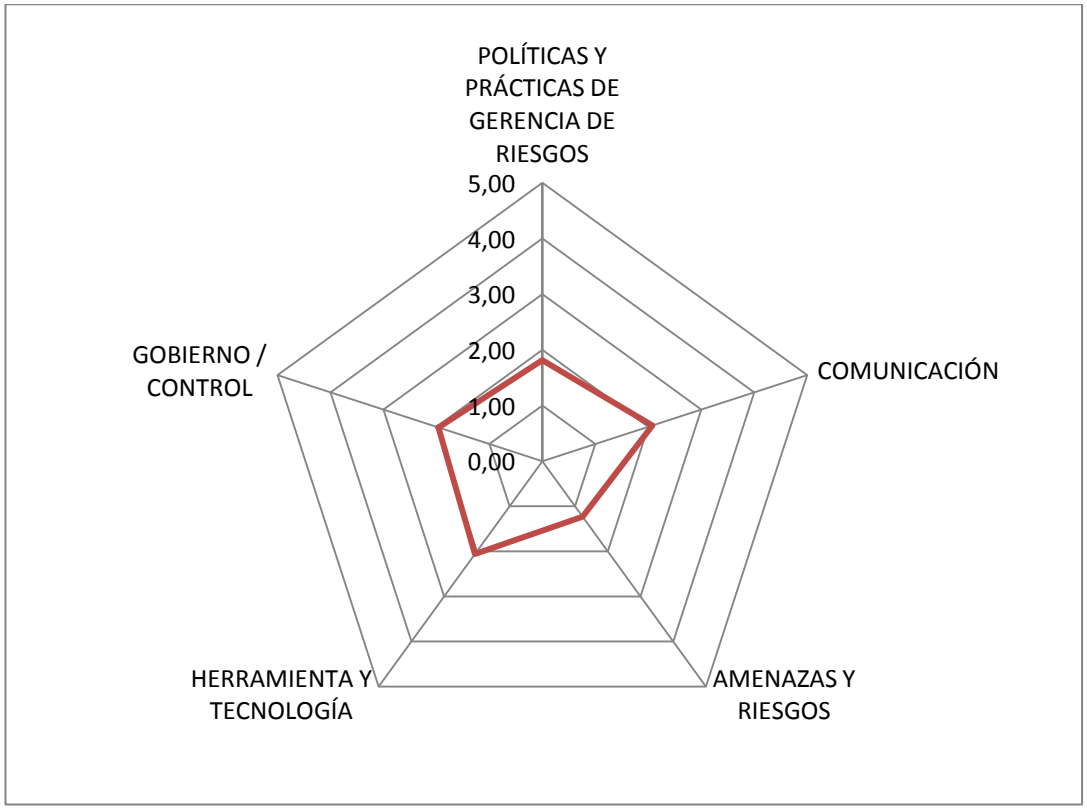


Figura 5. Diagrama de radar del nivel de madurez de gestión de riesgos tecnológicos en empresas ISP de la ciudad de Quito.

3.4. Conclusión

En función de los resultados mostrados (y cuyo detalle se presenta en el Anexo 2) se determina que la gestión de riesgos tecnológicos en empresas proveedoras del servicio de Internet (ISP) de la ciudad de Quito no se encuentra implementada en el nivel y madurez con el que se requeriría en una organización cuyo objetivo primordial del negocio depende directamente de la tecnología. Se considera necesario que los ISP tomen conciencia de la importancia que representa para sus objetivos de negocios el implementar una gestión integral de riesgos tecnológicos.

CAPITULO IV

PROPUESTA METODOLÓGICA PARA GESTIONAR RIESGOS TECNOLÓGICOS

4.1. Introducción.

En la actualidad, las organizaciones requieren de metodologías para administrar el riesgo tecnológico con el fin de proteger sus activos de información y evitar un paro parcial o total en sus procesos operativos. Es común encontrar en las organizaciones la falta de una cultura de gestión de riesgos, muchas de ellas suelen resolver sus incidentes luego de haber ocurrido, presentándose daños o pérdidas y en muchos casos la recuperación suele ser costosa.

Los ISP son organizaciones encaminadas a brindar sus servicios a la comunidad y la tecnología desempeña una función fundamental en los objetivos del negocio. Sin embargo, la constante innovación desencadena una serie de riesgos y esto exige un tiempo de reacción rápida por parte de estas empresas.

En base a las diversas metodologías que abarcan el tema de riesgos y mediante un análisis de las mismas, se considera diferentes aspectos esenciales para plantear una propuesta metodológica que permita gestionar los riesgos tecnológicos, dirigida hacia las empresas del sector de las telecomunicaciones, especialmente hacia los ISP.

4.2. Estructura

En el siguiente gráfico, y como una referencia general, se muestra el proceso de la gestión de riesgos en el que se destacan las entradas o insumos necesarios y las salidas o productos que se obtienen de esa gestión.

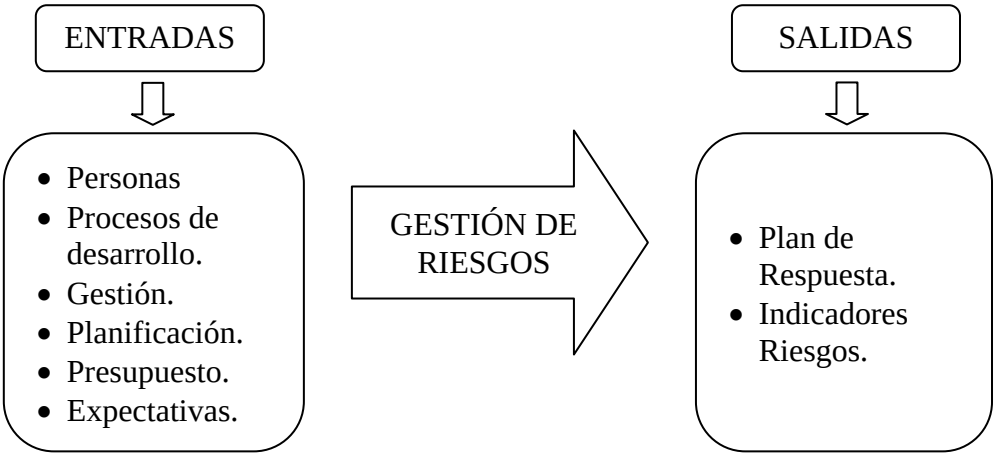


Figura 6. Visión general de la propuesta metodológica. Relación: Entradas / Salidas

La propuesta metodológica que se desarrollará en el presente estudio para la gestión de riesgos tecnológicos se basa en cuatro fases principales. A continuación se detallan dichas fases y las actividades a seguir dentro de cada una.

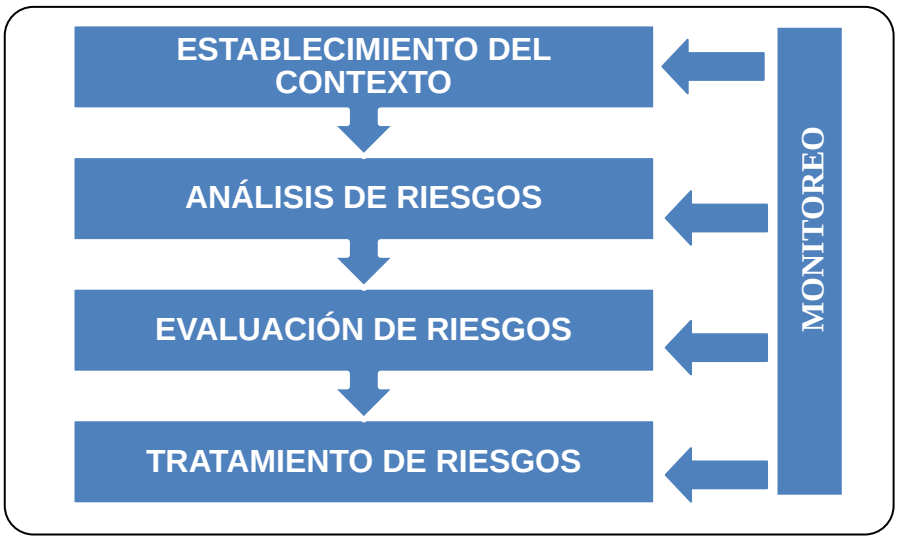


Figura 7. Fases generales de la propuesta metodológica planteada.

Establecimiento del contexto.- Condiciona aquello que la organización desea alcanzar y aquello de lo que la organización necesita protegerse. Se trata de organizar el trabajo y obtener el apoyo por parte de la empresa. Dentro del contexto se puede considerar dos aspectos: el entorno externo y el interno.

Se necesita una fuerte comprensión del entorno externo, a escala de la organización, para asegurar que el alcance del proceso de gestión del riesgo es coherente, especialmente, con:

- Las exigencias legales y reglamentarias, donde los riesgos de incumplimiento pueden poner en jaque a la organización.
- Las exigencias y presiones de clientes, proveedores, agentes sociales, personas, u otros grupos de interés, que pueden condicionar el sostenimiento del negocio.
- Otros aspectos de riesgos específicos que se consideren vinculados con factores claves o críticos de éxito de la organización (según su propia estrategia).

Por su parte, el contexto interno está constituido por todo aquello que puede influir en la manera en que se podrá gestionar el riesgo. Por ello, se deberían al menos considerar aspectos como:

- La estrategia, política y objetivos de la organización, ya que el alcance y los objetivos de la gestión del riesgo deben estar alineados con los primeros.
- La estructura, funciones y responsabilidades, pues la organización del proceso se efectúa en este marco.
- Los conocimientos, recursos y capacidades disponibles, ya que pueden ser restricciones o fortalezas para luego abordar la apreciación del riesgo en determinadas áreas, y las normas, directrices y modelos ya adoptados en la organización, que en definitiva marcan los procedimientos y métodos actuales de trabajo.

Análisis de riesgos.- Evidencia las vulnerabilidades que puedan ser explotadas por amenazas, provocando impactos en los negocios de la organización.

En un análisis de riesgos se pretende, a través del rastreo, identificar el riesgo a los cuales los activos tecnológicos se encuentran expuestos.; es decir, determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Evaluación de riesgos.- La evaluación de riesgos proporciona la información necesaria para decidir si los riesgos son aceptables o no aceptables. De esta forma se clasifican los riesgos más importantes para identificar las prioridades que se deberán considerar en la gestión.

Tratamiento de los riesgos.- Refiere a la implantación de mecanismos para gestionar los riesgos. Necesita ser adecuado o apropiado de acuerdo con la significancia del riesgo y la importancia del sector afectado. En esta fase, de manera general, se pueden considerar los siguientes criterios fundamentales:

- Riesgos de bajo nivel pueden ser aceptados y puede no ser necesaria una acción adicional sobre estos.
- Los riesgos de niveles significativos o más importantes deben ser necesariamente tratados.
- Los riesgos de altos niveles requieren de una cuidadosa administración o gestión, además del desarrollo de un plan formal para administrarlos.

4.3. Actividades y tareas.

A continuación se detallan las fases, actividades y tareas de la propuesta metodológica para la gestión de riesgos tecnológicos planteada.

FASE 1. Establecimiento del contexto

EC1: Planificación.

EC1.1 Situación actual de la empresa.

EC1.2 Determinar alcance.

EC1.3 Definir Plan de Trabajo.

EC2: Aprobación del Proyecto.

EC2.1 Aprobación por el Departamento de Tecnología.

EC2.2 Aprobación de la Gerencia.

EC3: Comunicación del proyecto.

FASE 2. Análisis de riesgos

AR1: Identificación de riesgos

AR1.1 Identificación de los activos

AR1.2 Identificación de las amenazas

AR1.3 Identificación de controles existentes

AR1.4 Identificación de las vulnerabilidades

AR2: Estimación de riesgos

AR2.1 Metodologías para la estimación del riesgo

AR2.2 Valoración de los incidentes (probabilidad).

AR2.3 Valoración de las consecuencias (impacto)

AR2.4 Nivel de estimación del riesgo (probabilidad vs impacto)

FASE 3. Evaluación de Riesgos

ER1: Evaluación y Priorización de riesgos.

ER1.1 Listado con los riesgos priorizados.

FASE 4. Tratamiento de Riesgos

TR1: Responder al Riesgo.

TR1.1 Identificar opciones de tratamiento.

TR1.2 Preparar planes de tratamiento.

TR1.3 Implementación.

4.4. Descripción de las actividades y tareas.

4.4.1. FASE 1: Establecer el contexto.

4.4.1.1. Actividad EC1: Planificación.

El objetivo en esta actividad es definir el pan de trabajo de la gestión de riesgos tecnológicos sobre la base del contexto, situación y recursos de la empresa. A continuación se describe las tareas de la presente actividad:

- **TAREA EC1.1 Información de la empresa.**

Se debe conocer el negocio de la empresa, sus objetivos y su participación en el mercado, así como el aporte que tiene las tecnologías dentro de la misma. Es fundamental conocer la cultura de riesgos que existe dentro de la organización ya que la dirección suele conocer de la innovación pero no de los problemas que estos implican.

Tabla 12

Tarea para recopilación de información de la empresa.

OBJETIVOS:

- **Definir a la organización considerando el ambiente externo y ambiente interno sobre el que opera.**
- **Identificar el interés de parte de la dirección o gerencia en la ejecución de una evaluación de riesgos tecnológicos.**

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Misión, visión y objetivos estratégicos. - Organigrama: estructura con funciones y responsabilidades. - Las exigencias normativas y reglamentos.	- Situación actual de la empresa. - Cultura de riesgo dentro de la organización.
TÉCNICAS Y PRACTICAS	
- Reuniones y Entrevistas - Cuestionarios macro	
PARTICIPANTES	
- Promotor(es) del proyecto - Responsable de TI - Responsable de cada área de la organización	

- **TAREA EC1.2. Determinar el alcance.**

Determinar el alcance es de vital importancia previo a la planificación sólida y consistente de la gestión de riesgos tecnológicos. El alcance implica establecer a detalle sus limitaciones, las normativas en las que se fundamenta, los involucrados directos e indirectos para su cumplimiento, las dimensiones, magnitudes y costos involucrados.

Tabla 13

Tarea para determinar el alcance.

OBJETIVOS:

- **Definir los objetivos del proyecto.**
- **Determinar las áreas y procesos sobre los cuales se realizará el análisis y evaluación de riesgos tecnológicos.**
- **Conocer la asignación clara de responsabilidades y recursos.**

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Plan estratégico de la empresa. - Mapa de procesos. - Políticas de seguridad implementadas. - Mapa de Riesgos - Gestión administrativa(estructura)	- Especificación del alcance.
TÉCNICAS Y PRACTICAS	
- Reuniones y Entrevistas - Análisis de requerimientos	
PARTICIPANTES	
- Promotor(es) del proyecto - Responsable de TI	

- **TAREA EC1.3. Definir el plan de trabajo.**

El plan de trabajo permite ordenar y sistematizar información relevante para la ejecución del proceso de gestión de riesgos. Sobre la base de la información recabada de las Tareas EC 1.1 y EC 1.2, se requiere diseñar un plan de trabajo que principalmente defina el calendario de cumplimiento de las distintas etapas, actividades y tareas del proyecto de gestión de riesgos.

Por su naturaleza, el plan de trabajo deberá desarrollarse en continua comunicación e interacción con los responsables de cada proceso; y por consiguiente, considerará la disponibilidad de recursos (técnicos, administrativos, humanos, etc.).

Tabla 14
Tarea para definir el plan de trabajo.

OBJETIVOS:

- **Diseñar el plan de trabajo en base a la información recopilada en tareas anteriores.**
- **Definir el respectivo calendario de realización de las distintas etapas, actividades y tareas del proyecto de gestión de riesgos tecnológicos.**
- **Establecer fechas de entrega de productos y modificaciones.**

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Especificación del alcance - Recursos por parte de la empresa	- Plan de trabajo detallado.

TÉCNICAS Y PRACTICAS

- Procesamiento de información
- Planificación de proyectos

PARTICIPANTES

- Promotor(es) del proyecto

4.4.1.2. ACTIVIDAD EC2: Aprobación del proyecto.

La aceptación y aprobación del plan de gestión de riesgos tecnológicos es de vital importancia para conseguir el apoyo mediante diferentes recursos por parte de la Gerencia.

- **TAREA EC2.1 Aprobación por parte del Departamento de Tecnología de la Información.**

El plan de trabajo debe ser aceptado por el departamento de TI, debido al soporte que brindan a los procesos de la organización es fundamental que estén de acuerdo hasta donde se planea llegar tanto en el alcance como en las actividades del plan de trabajo.

Tabla 15

Tarea para aprobación por parte del Departamento de TI.

OBJETIVOS:

- **Obtener el visto bueno por parte del departamento de TI para la presentación del proyecto ante la Gerencia General.**

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Plan de trabajo - Determinación del alcance	- Aceptación por parte de TI.

TÉCNICAS Y PRACTICAS

- Reunión con TI
- Exposición del plan de Gestión de Riesgos Tecnológicos

PARTICIPANTES

- Promotor(es) del proyecto
- Departamento de TI

- **TAREA EC2.2 Aprobación por parte de la Gerencia.**

Es necesario que la gerencia conozca la importancia de la gestión de riesgos tecnológicos dentro de la organización debido a la gran dependencia de la tecnología dentro de la misma. La gerencia debe conocer los objetivos, el propósito, así como el alcance del proyecto con el fin de lograr su aprobación y dar inicio al plan de Gestión de Riesgos.

Tabla 16

Tarea para aprobación por parte de la Gerencia.

OBJETIVOS:

- **Presentar el plan de Gestión de Riesgos tecnológicos ante la Gerencia General.**
- **Obtener la carta de aprobación para dar inicio al proyecto.**

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Plan de trabajo - Determinación del alcance - Aceptación por parte de TI.	- Aprobación de Gerencia para la ejecución.

TÉCNICAS Y PRACTICAS

- Reunión con gerencia
- Exposición del plan de Gestión de Riesgos Tecnológicos

PARTICIPANTES

- Promotor(es) del proyecto
- Departamento de TI
- Gerencia General

4.4.1.3. ACTIVIDAD EC3: Comunicación.

Esta actividad consiste en lanzar una campaña informativa a los implicados necesarios sobre el inicio y aporte que deben tener dentro del proyecto.

- **TAREA EC3.1 Presentación y comunicación del proyecto.**

En esta etapa la comunicación a las áreas y personal de la organización respecto al proceso de Gestión de Riesgos Tecnológicos busca obtener el apoyo necesario para agilizar y optimizar la ejecución del mismo.

Tabla 17

Tarea para presentación y comunicación del proyecto.

OBJETIVOS:

- **Informar sobre la cooperación que debe tener el personal o áreas de la organización involucrados dentro de la ejecución de la Gestión de Riesgos Tecnológicos.**
-

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Plan de Gestión de Riesgos Tecnológicos - Aprobación de la Gerencia	- Conocimiento y apoyo de los involucrados

TÉCNICAS Y PRACTICAS

- Exposiciones o charlas.
- Memorandos.

PARTICIPANTES

- Promotor(es) del proyecto.
- Áreas o personal involucrados.

4.4.2. FASE 2: ANÁLISIS DE RIESGOS

4.4.2.1. ACTIVIDAD AR1: Identificación de riesgos.

Una organización al disponer y depender de medios de tecnología así como sistemas de información, trae consigo una serie de riesgos conocidos como tecnológicos, los mismos que puede provocar una pérdida potencial dentro de la entidad, por esta razón la gestión de riesgos cumple un papel crítico que le permita a la organización identificar dichos riesgos y así poder hacerlos frente con el propósito de evitar daños o pérdidas en los activos del negocio. A continuación se describe las tareas de la presente actividad:

- **TAREA AR1.1 Identificación de los activos.**

Es fundamental disponer de un inventario de activos tecnológicos, partiendo desde los datos, su emisor, el medio en que transmite, almacena y hasta su receptor final. Dentro del grupo tecnológico podemos mencionar:

- Activos primarios, específicamente relacionados con los procesos de la empresa.

- Activos tangibles, aquellos relacionados con: la infraestructura física; y, la información (del negocio, comercial, financiera, personal, etc.)

- Activos intangibles: relacionados con la marca, reputación, productividad, ambiente laboral, experiencia, posicionamiento, etc.

- Servicios de TI: principalmente aquellos activos directamente relacionados con la infraestructura de Core, con servicios de mensajería, además de aplicaciones, software, etc.

En el Anexo 4 se presenta el lineamiento bajo el cual la presente propuesta metodológica para la gestión de riesgos establece la identificación de activos.

Tabla 18

Tarea para identificación de los activos.

OBJETIVOS:

- **Determinar los activos tecnológicos relevantes para la organización.**
- **Valorar los activos según el grado de criticidad.**

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Alcance. - Lista de componentes con sus propietarios. - Ubicación y funciones de los componentes.	- Lista de activos que se someterán a la evaluación. - Procesos relacionados con esos activos.
TÉCNICAS Y PRACTICAS	
- Reuniones - Entrevistas	
PARTICIPANTES	
- Promotor(es) del proyecto - Responsables de TI - Propietarios de la información	

- **TAREA AR1.2 Identificación de amenazas.**

Una vez recopilada la información necesaria para la comprensión del negocio así como los activos tecnológicos que están involucrados, se define un mapa o catálogo de amenazas bien identificadas, lo más completo posible, considerando, tanto amenazas internas como externas, factores humanos y acciones accidentales, ambientales, etc.

Es importante mirar diferentes fuentes que permitan considerar las posibles amenazas para el entorno en el cual se enfoque, por ejemplo; existen metodologías que presentan varias categorías de amenazas hacia los activos tecnológicos, así

también se recopila datos estadísticos sobre posibles amenazas que se han reportado dentro de la empresa. Otra fuente fundamental es a nivel organizacional, es decir la manera como se lleva la gestión de tecnología y su relación con los procesos del negocio.

En ese sentido, el listado de amenazas de la propuesta metodológica que se presenta toma como referencia el catálogo de amenazas establecidas por la metodología MAGERIT V3.

Otro aspecto a considerar es el mantener actualizado este escenario de amenazas debido a que las mismas muchas veces son variantes de otras anteriores y pueden surgir nuevas.

MAPA DE AMENAZAS (referencia):

- *DE ORIGEN INDUSTRIAL*
  - Fuego
  - Daños por agua
  - Explosiones, sobrecarga eléctrica, etc.
  - Contaminación mecánica
  - Contaminación electromagnética
  - Avería de origen físico o lógico
  - Corte del suministro eléctrico
  - Condiciones inadecuadas de temperatura
  - Fallo de servicios de comunicaciones
  - Interrupción de otros servicios y suministros esenciales
  - Degradación de los soportes de almacenamiento de la información

- *ERRORES Y FALLOS NO INTENCIONADOS*
  - Errores de los usuarios
  - Errores del administrador
  - Errores de monitorización (log)

- Deficiencias en la organización
- Difusión de software dañino
- Errores de [re-]encaminamiento
- Escapes de información
- Alteración accidental de la información
- Destrucción de información
- Fugas de información
- Vulnerabilidades de los programas (software)
- Errores de mantenimiento / actualización de programas (software)
- Errores de mantenimiento / actualización de equipos (hardware)
- Caída del sistema por agotamiento de recursos
- Pérdida de equipos

- *ATAQUES INTENCIONADOS*
  - Manipulación de los registros de actividad (log)
  - Manipulación de la configuración
  - Suplantación de la identidad del usuario
  - Abuso de privilegios de acceso
  - Difusión de software dañino
  - Alteración de secuencia
  - Acceso no autorizado
  - Repudio
  - Interceptación de información (escucha)
  - Destrucción de información
  - Divulgación de información
  - Manipulación de programas
  - Manipulación de los equipos
  - Denegación de servicio
  - Robo
  - Ataque destructivo
  - Extorsión
  - Ingeniería social (picaresca)

- *INSTITUCIONALES*
  - Proyectos nuevos de tecnología mal ejecutados
  - Adquisición de tecnología sin previo análisis
  - Personal con conocimiento desactualizado
  - Indisponibilidad del personal
  - Mal uso de Internet y otros recursos tecnológicos.

Tabla 19

Tarea para identificación de amenazas.

OBJETIVOS:

- **Identificar las diversas amenazas que podrían materializarse afectando a los activos relacionados.**

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Mapa amenazas referencial (Ej. Inventario de amenazas MAGERIT V3) - Amenazas obtenidas de propietarios, usuarios e incidentes registrados.	- Amenazas con el tipo y origen

TÉCNICAS Y PRACTICAS

- Reuniones.
- Análisis de información.

PARTICIPANTES

- Director del Proyecto.
- Promotor(es) del proyecto

- **TAREA AR1.3 Identificación de controles existentes.**

Sobre la base del mapa de amenazas e información recabada de reuniones y entrevistas con los propietarios y responsables de los activos, se identifican los controles que se encuentren implementados.

Para el efecto se recurrirá principalmente a la revisión de políticas y procedimientos (definidos y difundidos), elementos de control en operación, planes de tratamiento de riesgos ejecutados, evaluaciones previas; y toda demás información que permita al equipo evaluador determinar los controles existentes y su estado de implementación. Adicionalmente pueden ser útiles tanto los informes de implementación de controles de planes de tratamiento de riesgos anteriores así como informes de auditoría. Deben considerarse tanto los controles existentes como aquellos incluidos en el Plan de Tratamiento de Riesgos si lo tuviesen.

Tabla 20

Tarea para identificación de controles existentes.

OBJETIVOS:

- **Identificar los controles implementados**

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Mapa de amenazas. - Políticas, procedimientos, estructuras de control - Planes de tratamiento de riesgos implementados - Evaluaciones de control interno y su implementación	- Controles implementados. - Estado de implementación y uso.
TÉCNICAS Y PRACTICAS	
- Reuniones - Entrevistas	
PARTICIPANTES	
- Promotor(es) del proyecto - Responsable de TI	

- **TAREA AR1.4 Identificación de vulnerabilidades.**

El objetivo de este punto es detectar las vulnerabilidades que se encuentran dentro de la organización, tras las debidas reuniones con el personal involucrado para obtener los controles existentes, junto con las amenazas identificadas y toda la demás información adicional que el equipo evaluador considere pertinentes, como por ejemplo: Informes internos de vulnerabilidades (de existir), vulnerabilidades conocidas, análisis de reportes de incidentes, inventario de activos, etc.

Si se detectaran vulnerabilidades que no provienen de una amenaza conocida, debe documentarse, debido a que el escenario y las amenazas podrían cambiar. Se obtiene entonces una lista de vulnerabilidades de los activos, considerando siempre las amenazas y controles existentes.

Tabla 21

Tarea para identificación de vulnerabilidades.

OBJETIVOS:

- Identificar las vulnerabilidades presentes en la organización (procesos, dispositivos tecnológicos, sistemas informáticos, entre otros).

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Mapa de amenazas. - Inventario de activos. - Controles existentes.	- Vulnerabilidades relacionadas con los activos y mapa de amenazas. - Vulnerabilidades sin relación con amenazas identificadas.
TÉCNICAS Y PRACTICAS	
- Reuniones. - Entrevistas. - Análisis de información.	
PARTICIPANTES	
- Promotor(es) del proyecto.	

4.4.2.2. ACTIVIDAD AR2: Estimación de riesgos

En la presente actividad se considerarán las metodologías de estimación de riesgos, así como la valoración de la probabilidad de ocurrencia y del impacto de amenazas. A continuación se describen las correspondientes tareas:

- **TAREA AR2.1 Metodologías para la estimación del riesgo.**

La metodología para la estimación puede ser cualitativa o cuantitativa; incluso una combinación de ambas. La selección de una de ellas depende principalmente de cuan críticos son los activos a proteger, de las vulnerabilidades detectadas y del nivel de gestión de riesgos que tenga la empresa.

Como se conoce, una estimación cualitativa utiliza una escala de rangos de valores, sobre la cual recaen las magnitudes (ya sean de probabilidad o de impacto). Su principal ventaja es el alto grado de comprensión que se puede lograr por parte del personal involucrado, situación que coadyuva al cumplimiento de los objetivos fijados para la evaluación. En contra parte, se encuentra cierta subjetividad en la selección de las respectivas escalas.

La estimación cuantitativa utiliza una escala con valores numéricos para la determinación de probabilidades y consecuencias; y, en la mayoría de los casos, utiliza datos históricos respecto de los correspondientes incidentes; lo que conlleva a conseguir una estimación mucho más precisa. La desventaja radica principalmente en la falta de dichos datos históricos pudiendo crear un efecto de “ilusión del valor y la exactitud de la valoración del riesgo”, como lo define la norma ISO/IEC 27005:2012.

En ese sentido, esta misma norma recomienda que, en función de prácticas más frecuentes, en primera instancia se utilice una estimación cualitativa para obtener un panorama general del nivel de riesgo; y posteriormente podría ser necesario un análisis de tipo cuantitativo de aquellos riesgos importantes.

Es decir, en el caso de riesgos que podrían afectar significativamente los resultados, la valorización cualitativa se utiliza como una evaluación inicial para identificar situaciones que ameriten un estudio más profundo.

Con ese antecedente; en esta instancia resulta pertinente retomar los resultados de la investigación efectuada en el Capítulo III del presente trabajo: “CULTURA DE ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS EN ISP DEL DISTRITO METROPOLITANO DE QUITO” en la cual se obtuvo que el nivel de madurez en la gestión de riesgos tecnológicos de los ISP en la ciudad de Quito, se encuentra por debajo del nivel administrable en cada uno de los dominios evaluados:

- Políticas y prácticas de gerencia de riesgos: 1.81 / 5
- Comunicación: 2.08 / 5
- Amenazas y riesgos: 1.23 / 5
- Herramienta y tecnología: 2.06 / 5
- Gobierno y control: 1.96 / 5

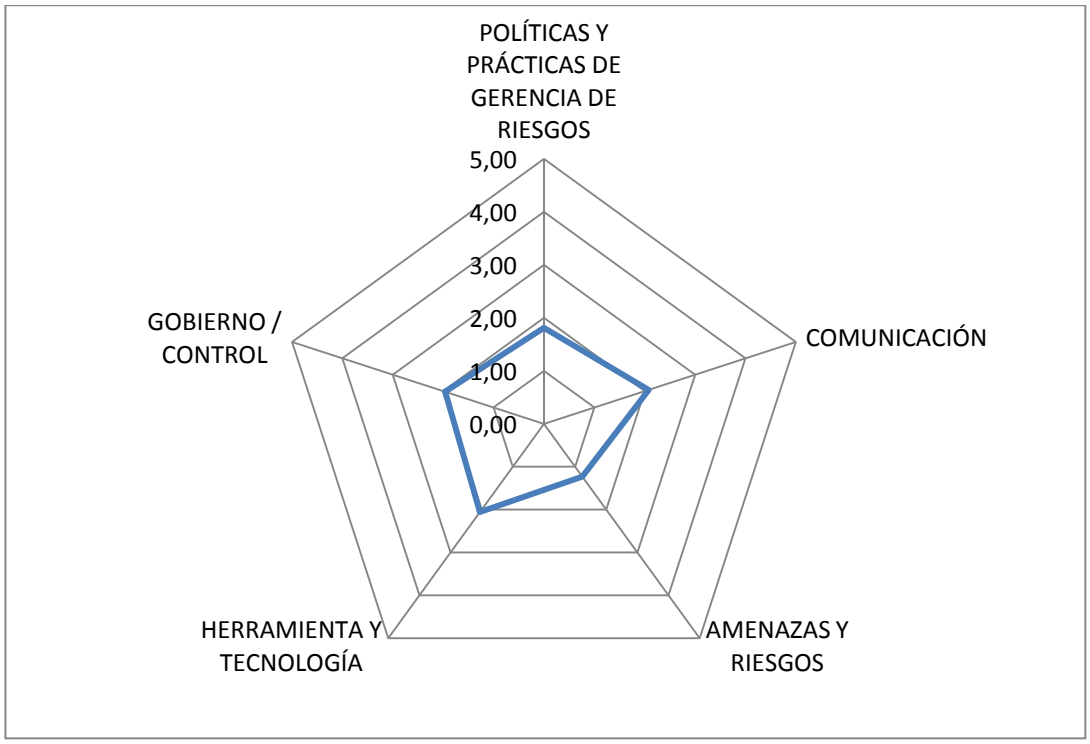


Figura 8. Diagrama de radar del nivel de madurez de gestión de riesgos tecnológicos en empresas ISP de la ciudad de Quito.

Adicionalmente, a partir de dicha investigación se pueden hacer referencia a los siguientes principales resultados:

- El 84.62% de los ISP encuestados manifestaron no poseer una política formal, implementada a la fecha, para la administración de riesgos tecnológicos.

- El 46.15% de los ISP encuestados indicaron no tener implementado ningún proceso de administración de riesgos en sus empresas; y no tenerlo previsto.

- El 61.54% de los ISP indicó no tener ninguna iniciativa en firme para implementar algún marco de referencia (Ej., COBIT, ISO27005, MAGERIT, etc.).

- El 53,85% de los ISP contactados, hasta la fecha, no han ejecutado una evaluación de riesgos tecnológicos; aunque el 15,38% de ellos lo tendría planificado.

Por lo tanto, considerando dichos niveles de gestión de riesgos en las empresas ISP de la ciudad de Quito (por debajo del nivel administrable), y acogiendo lo que se manifiesta en la norma ISO/IEC 27005:2012, para la presente metodología se efectuará mayor énfasis en una estimación de riesgos cualitativa; cuyas escalas se detallarán en cada una de las tareas a ejecutar.

Con el objetivo de minimizar la subjetividad a la que está sujeta por naturaleza la estimación cualitativa, se establecerán criterios de calificación que bien podrán ser adoptadas en la aplicación de esta propuesta metodológica y que se detallan también en cada una de las tareas de valoración respectivas.

Finalmente, si una empresa en particular considera que sus niveles de gestión de riesgo son administrables y que además cuenta con información de evaluaciones anteriores; o, considera una alta criticidad de sus activos y que maneja amplias vulnerabilidades, lo recomendable sería definir una metodología de estimación de

riesgos cuantitativa; basada en las mismas tareas que esta propuesta metodológica plantea.

Tabla 22

Tarea para definir metodologías para la estimación del riesgo

OBJETIVOS:

- Definir la metodología más idónea que permita la estimación del grado de exposición a que un riesgo se materialice sobre uno o más activos.

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Plan de trabajo - Cultura y madurez de gestión de riesgos	- Determinación de la metodología (cualitativa / cuantitativa)
TÉCNICAS Y PRACTICAS	
- Reuniones - Análisis de información	
PARTICIPANTES	
- Promotor(es) del proyecto	

- **TAREA AR2.2 Valoración de la probabilidad.**

Esta tarea tiene por objetivo determinar las probabilidades latentes de que las diferentes amenazas se puedan materializar. Es decir, debe analizarse qué tan probable resulta que las amenazas identificadas exploten las vulnerabilidades.

La probabilidad de ocurrencia establece la posibilidad de que una o varias amenazas identificadas puedan explotar su vulnerabilidad asociada, debido a la falta de controles o la ineficiencia de los controles implementados. Para la estimación de dicha probabilidad se requerirán como insumos la identificación de activos, amenazas, controles existentes y de vulnerabilidades; a fin de desarrollar una matriz de la frecuencia o probabilidad estimada para cada uno de los riesgos identificados.

La valoración, como se explica en la tarea AR 2.1., se podrá estimar a través de un método cualitativo en el que se definirán las escalas que se muestran a continuación.

Tabla 23
Probabilidades de ocurrencia de riesgo.

PROBABILIDADES DE OCURRENCIA DE RIESGO	
ESCALA	**VALOR**
ALTA	4
MODERADA	3
MEDIA	2
BAJA	1
NINGUNA	0

El uso de escalas como la mostrada en la Tabla 23, de acuerdo a los autores: Dr. David Hillson y Dr. David T. Hulett, en su publicación “Calculando probabilidades de riesgos: Métodos alternativos”, corresponde a una “técnica definitoria” para la estimación de probabilidades de riesgos que posee ciertos problemas de efectividad por su fundamento en la utilización de frases o términos ambiguos, Ej.: “Muy frecuente”, “Frecuente”, “Ocasional”, etc.

En ese sentido, los mismos autores refieren a otro método denominado de “Estado Natural”, el que principalmente se basa en la descripción específica de un rango de situaciones o escenarios los cuales tienen una probabilidad de riesgos asociada. Es decir, que la situación o incidente se compara con un conjunto definido y objetivo de alternativas.

Así, dichas alternativas corresponderán a los siguientes criterios de estimación a utilizarse en la presente propuesta metodológica y que podrían redefinirse de acuerdo a los requerimientos de cada empresa:

Tabla 24

Criterios para estimación de probabilidad.

ESCALA	ESTADO NATURAL
ALTA	Probabilidad de ocurrencia del riesgo al no existir controles que impidan el desarrollo del incidente o ataque. La materialización de la amenaza es inminente.
MODERADA	Probabilidad de ocurrencia del riesgo ante controles cuya implementación no se encuentra documentada y/o demostrada durante evaluación.
MEDIA	Probabilidad de ocurrencia del riesgo ante controles implementados con documentación inadecuada y/o incompleta.
BAJA	Probabilidad de ocurrencia del riesgo ante controles implementados y que se encuentran documentados, difundidos y/o monitoreados.
NINGUNA	No existen condiciones que impliquen riesgo.

Es muy importante destacar que para este particular, la probabilidad de ocurrencia de un riesgo se valora en función del estado de los controles que tenga implementados la empresa. Es decir, corresponde a la probabilidad de un **riesgo residual** que permanece después de las direcciones establecidas por la empresa. Entonces por lo tanto, se trata de la probabilidad de un **RIESGO RESIDUAL ACTUAL**.

Finalmente, una estimación de probabilidad cuantitativa es factible preferentemente si existe información o datos de probabilidad de ocurrencia de amenazas provenientes de alguna evaluación, monitoreo o gestión de riesgos aplicado anteriormente, a efecto de aplicar una estimación de tipo comparativa.

Tabla 25

Tarea para valorar la probabilidad.

OBJETIVOS:

- Determinar las probabilidades de que las amenazas se materialicen y la facilidad en las que las vulnerabilidades pueden ser explotadas.

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Identificación de activos. - Identificación de amenazas. - Identificación de controles existentes. - Identificación de vulnerabilidades.	- Probabilidad estimada para cada uno de los riesgos identificados
TÉCNICAS Y PRACTICAS	
- Reuniones - Análisis de información	
PARTICIPANTES	
- Promotor(es) del proyecto	

- **TAREA AR2.3 Valoración de las consecuencias (impacto)**

El equipo participante en el proyecto es responsable de valorar el impacto de daño o pérdida en los activos de la empresa. Para esta tarea es primordial tener bien definida la identificación de activos clasificados por grupos. Tanto para evaluar el impacto, probabilidad y riesgo se puede utilizar escalas cualitativas. Por ejemplo, MAGERIT versión 3 plantea la siguiente escala:

Tabla 26

Escalas en otros marcos de referencia.

• MB:	**Muy bajo**
• B:	Bajo
• M:	Medio
• A:	Alto
• MA:	Muy alto

Fuente: MAGERIT v. 3.0

Sin embargo, siguiendo con el método de “Estado Natural” definido por los autores Dr. David Hillson y Dr. David T. Hulett, en su publicación “Calculando probabilidades de riesgos: Métodos alternativos”, para la presente escala de evaluación de impacto se consideran los siguientes criterios según la magnitud de alteración que pueda ocurrir en los activos tecnológicos de la organización y el daño que pueda suceder en el negocio.

Tabla 27

Criterios para valoración de Impacto.

NIVEL	CATEGORÍA	CRITERIO
4	Muy alto	La magnitud de daño es perjudicial para la organización, puede ocasionar importantes pérdidas debido a que el negocio depende 100% de los activos tecnológicos que se ven afectados
3	Alto	El impacto es alto y la magnitud de daño puede influir de manera considerable a la organización provocando pérdidas en tiempo y dinero.
2	Medio	Impactos de magnitud media que pueden ser tratados o pasar desapercibidos si el daño estimado no es perjudicial para la organización.
1	Bajo	Impactos que no son de consideración ya que la magnitud o dimensión de alteraciones dentro de la organización no afectan al negocio.
0	Muy Bajo	No presenta ninguna alteración ni cambios negativos en los activos tecnológicos de la organización que puedan afectar a los procesos y servicios del negocio.

Tabla 28

Tarea para valorar las consecuencias (Impacto)

OBJETIVOS:

- **Evaluar las consecuencias relacionadas con los activos y criterios de impacto.**
- **Valorar el impacto de un escenario considerando como factor clave la valoración de activos.**

PRODUCTOS DE ENTRADA	**PRODUCTOS DE SALIDA**
- Lista de escenarios de incidentes con sus consecuencias relacionadas con los activos tecnológicos.	- Lista de las consecuencias valorada.

TÉCNICAS Y PRACTICAS
- Reuniones - Análisis de información

PARTICIPANTES
- Promotor(es) del proyecto

- **TAREA AR2.4 Nivel de estimación del riesgo (probabilidad vs impacto)**

Existe una variedad de métodos que se utilizan para calificar los riesgos y así conocer el grado de criticidad de los mismos. Es importante en la estimación del riesgo considerar dos variables; el impacto sobre daños a pérdidas que enfrente la organización cada vez que acurran las amenazas y la probabilidad de ocurrencia de las amenazas.

Tanto la probabilidad como el impacto mantienen su respectiva escala y el resultado de multiplicar estas dos variables resuelta en el nivel de riesgo (GTAG-11. Developing the IT Audit Plan, 2008):

[1] $$R = P \times I$$

Donde,

R: Score del riesgo.

P: Probabilidad.

I: Impacto.

Tabla 29

Tarea para medir el nivel de estimación del riesgo (probabilidad vs impacto).

OBJETIVOS:

- Asignar valores de probabilidad e impacto, valores que pueden ser cualitativos y cuantitativos.
- Estimar el riesgo en base a las consecuencias evaluadas y a la probabilidad.

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Probabilidad de un escenario de incidente. - Lista de consecuencias valorada (impacto)	- Lista de riesgos valorados.
TÉCNICAS Y PRACTICAS	
- Reuniones - Análisis de información	
PARTICIPANTES	
- Promotor(es) del proyecto	

El objetivo es proveer una matriz unificada de la probabilidad e impacto, con los valores establecidos de acuerdo a los activos tecnológicos como a los riesgos identificados.

La matriz “Probabilidad * Impacto” tendrá la estructura mostrada en la Tabla 30, basada en el concepto de evaluación del riesgo definida por la Guía de Auditoría de Tecnología Global GTAG-11. Developing the IT Audit Plan (2008).

Tabla 30

Cálculo: Probabilidad x Impacto

	Activo 1		**Activo 2**		**Activo 3**		**…**	**Activo n**		
RIESGOS	**P**	**I**	**P**	**I**	**P**	**I**		**P**	**I**	**P x I**
Riesgo$_1$	P_1	I_1	P_2	I_2	P_3	I_3		P_n	I_n	**R**
Riesgo$_2$										
…										
Riesgo$_m$										

[2] $$\mathbf{R = (P_1 \times I_1) + (P_2 \times I_2) + (P_3 \times I_3) + \ldots + (P_n \times I_n)}$$

Donde,

R: Score del riesgo.

P: Probabilidad de ocurrencia.

I: Impacto.

4.4.3. FASE 3: EVALUACIÓN DE RIESGOS

4.4.3.1. ACTIVIDAD ER1: Evaluación y priorización de riesgos

Esta actividad ejecuta una evaluación de riesgos con el propósito de tener una visión clara sobre el nivel de los mismos dentro de la organización. El propósito de la visión es que se pueda decidir sobre la aceptabilidad o rechazo de los riesgos. A continuación se describe la tarea de la presente actividad:

- **TAREA ER1.1. Priorización de riesgos.**

Una vez identificados los riesgos de acuerdo al área y recursos tecnológicos dentro de la organización, es fundamental valorarlos y clasificarlos por orden de prioridad, esta clasificación servirá para buscar soluciones que permitan eliminar o prevenir los riesgos.

Tabla 31

Tarea para obtener la lista de riesgos priorizados.

OBJETIVOS:

- **Emplear técnicas de evaluación de riesgos identificados que rodean a la organización.**
- **Obtener una clasificación de riesgos según su prioridad.**

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Lista de riesgos valorados. - Criterios de evaluación del riesgo.	- Riesgos priorizados

TÉCNICAS Y PRACTICAS

- Reuniones
- Análisis y recopilación de información

PARTICIPANTES

- Promotor(es) del proyecto

La matriz con los riesgos valorados según la probabilidad e impacto es el punto de entrada principal para la priorización. La siguiente tabla permite establecer la clasificación según los riesgos valorados en la fase de análisis.

Tabla 32

Escala de riesgos priorizados.

ESCALA DE RIESGO PRIORIZADOS

Riesgo	Score	Nivel	Interpretación
Muy Alto	**151 - 200**	**4**	**Riesgos Intolerables**
Alto	**101 - 150**	**3**	**Riesgos Importantes**
Medio	**51 - 100**	**2**	**Riesgos Moderados**
Bajo	**1 - 50**	**1**	**Riesgos Bajos**

La interpretación permite clasificar y ordenar los riesgos y reestructurar la matriz de acuerdo al nivel de priorización.

4.4.4. FASE 4: TRATAMIENTO DE RIESGOS

4.4.4.1. ACTIVIDAD TR1: Respuesta al riesgo

Para responder al riesgo tecnológico siempre será necesario conocer la significancia del riesgo y la importancia de los procesos o activo de la organización. A continuación se describe las tareas de la presente actividad:

- **TAREA TR1.1 Identificar opciones de tratamiento.**

Las opciones serán función de evitar, mitigar, trasferir o aceptar el riesgo. Existen muchas opciones de tratamiento de riesgos tecnológicos que deben analizarse conforme las circunstancias y su interrelación (Por ejemplo, evitar inadecuadamente algunos riesgos puede aumentar la significación de otros si el tratamiento no es el correcto).

Tabla 33

Tarea para identificar opciones de tratamiento.

OBJETIVOS:

- Identificar las mejores alternativas para reducir o controlar el grado de ocurrencia según el nivel del riesgo tecnológico.
- Evaluar las opciones de tratamiento.

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Riesgos tecnológicos priorizados. - Activos de la organización.	- Listado con las opciones de tratamiento.

TÉCNICAS Y PRACTICAS

- Reuniones
- Análisis de información
- Análisis costo – beneficio

PARTICIPANTES

- Promotor(es) del proyecto

- **TAREA TR1.2. Preparar e implementar los planes de tratamiento.**

Es competencia de la empresa preparar los planes para la mitigación de riesgos, sobre la base de las recomendaciones que se deriven de la aplicación de la presente propuesta metodológica para la gestión de riesgos.

Tabla 34

Tarea para preparar los planes de tratamiento.

OBJETIVOS:

- Elaborar planes para reducir o controlarla probabilidad de la ocurrencia de los riesgos identificados.
- Evaluar costos y beneficios.

Continúa →

PRODUCTOS DE ENTRADA	PRODUCTOS DE SALIDA
- Riesgos tecnológicos priorizados. - Opciones de tratamiento de riesgos.	- Informe con los planes a efectuarse.
TÉCNICAS Y PRACTICAS	
- Reuniones - Análisis de información	
PARTICIPANTES	
- Gerencia y otros involucrados de la empresa.	

La consolidación de las fases y actividades y la representación de las entradas y salidas de cada una de las tareas, se presentan en el Anexo 3.

4.5. Evaluación de hipótesis

La hipótesis que se plantea en el presente estudio corresponde a la obtención de indicadores que permitan minimizar los riesgos tecnológicos dentro de una empresa proveedora del servicio de Internet (ISP). Para tal efecto, sobre la base del estudio desarrollado, se obtuvieron dos tipos de indicadores.

El primero, define una perspectiva global, que se basa en la consideración de los resultados obtenidos de la investigación realizada al nivel de madurez con que los ISP de la ciudad de Quito administran sus riesgos tecnológicos.

El siguiente escenario, establece una perspectiva individual, y se basa en la propuesta metodológica para gestión de riesgos que se plantea en el presente capítulo. A continuación las respectivas descripciones.

4.5.1. Indicadores desde diagrama de madurez.

De manera global, la investigación efectuada en el capítulo III determinó el grado de madurez con que los ISP de la ciudad de Quito administran sus riesgos tecnológicos, observándose esencialmente que los niveles alcanzados en cada uno de los dominios evaluados (Políticas y prácticas de gerencia de riesgos, Comunicación,

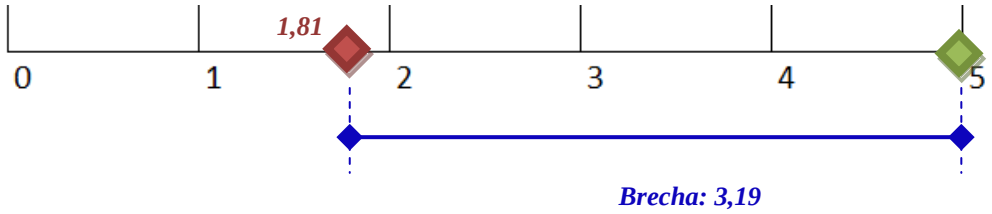
Amenazas y riesgos, Herramienta y tecnología; y, Gobierno y control) no alcanzan un grado que pueda ser considerado “Administrable”.

Como se observa por tanto, los resultados del nivel de madurez se convierten en indicadores con los cuales las empresas pueden identificar los dominios en los cuales requieren enfatizar medidas y correctivos.

Es decir, la representación del nivel inicial alcanzado corresponde a indicadores situacionales que identifican las brechas existentes para llegar a un nivel “Administrable”, constituyéndose en indicadores de madurez.

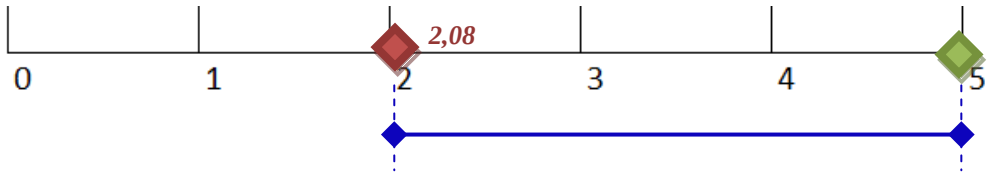
Así, se tiene que:

POLÍTICAS DE GERENCIA DE RIESGOS



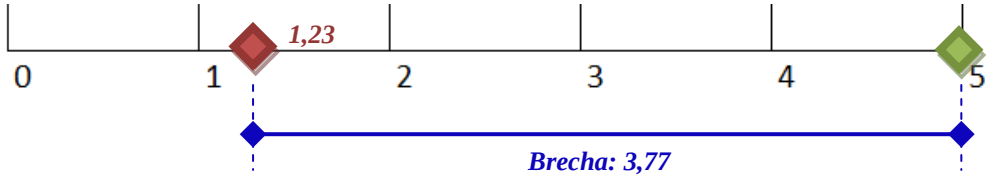
Brecha: 3,19

COMUNICACIÓN



Brecha: 2,92

AMENAZAS Y RIESGOS



Brecha: 3,77

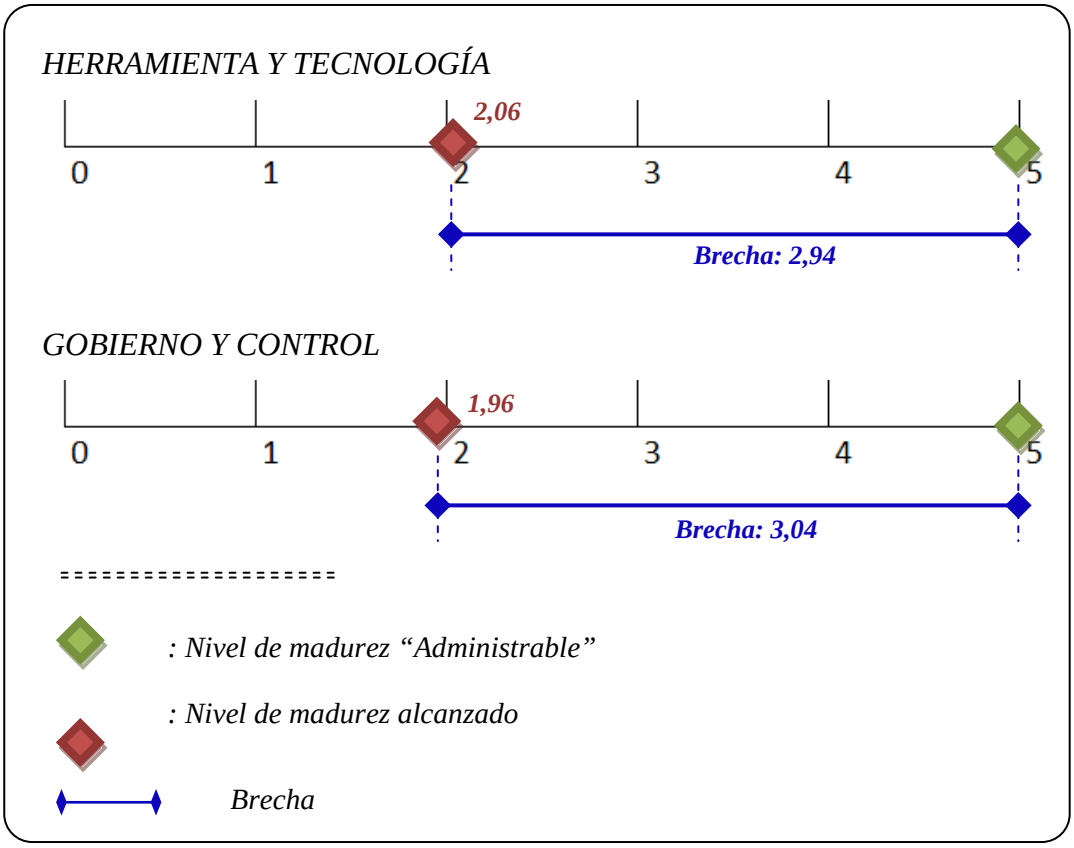


Figura 9. Indicadores. Brechas existentes para alcanzar el nivel "Administrable".

Pudiéndose por tanto establecer una priorización en los dominios en los cuales se requiere mayor atención:

a) Amenazas y riesgos.- Se requiere mayor atención hacia un programa integral de administración de riesgos (acoplado o en sincronía con las políticas y prácticas de la empresa) que permita a cada uno de los responsables (de áreas o procesos) percibir cambios en los ambientes de riesgos en función de la constante evolución de factores externos como la situación económica de la empresa, redes sociales, dispositivos personales, cómputo en nube, etc.; y retroalimentar las políticas y prácticas de gestión de riesgos vigentes.

b) Políticas y prácticas de gerencias de riesgos.- Se requiere el establecimiento de políticas formales para la administración de riesgos, que incluyan procesos documentados respecto de la implementación de algún marco de referencia (COBIT,

COSO, ISO, MAGERIT u OTRO); o, la adopción de algún manual de buenas prácticas en la gestión de riesgos; o en la medida de lo posible, la ejecución de una actividad de auditoría técnica en la empresa.

c) Comunicación.- Para atender esta brecha se requiere que dentro de la organización se emprendan campañas de difusión, capacitación, interiorización e incluso evaluación de las diferentes políticas establecidas (Políticas de seguridad de la información, políticas de comunicación interna y externa, políticas de seguridad industrial, etc.).

d) Gobierno / Control.- La empresa debe establecer una estructura organizacional acorde con las políticas de gestión de riesgos adoptadas. Los controles implementados y las evaluaciones que se decidan efectuar deben corresponder a planes formales de contingencia o de respuesta a incidentes.

e) Herramienta y tecnología.- Se requiere que la gestión de riesgos tecnológicos en la empresa se soporte en tecnología específica, como software o control específico de administración de accesos, identidades etc.

4.5.2. Indicadores tras la propuesta metodológica de gestión de riesgos.

Tal como se desarrolla en el presente capítulo, la propuesta metodológica para la gestión de riesgos en empresas ISP incluye fases, actividades y tareas destinadas, en conjunto, hacia una evaluación de riesgos tecnológicos que permita la obtención de indicadores sobre los cuales una determinada empresa pueda tomar decisiones y acciones de control.

En ese sentido, los indicadores que dicha propuesta metodológica arroja, corresponden a los RIESGOS PRIORIZADOS que se obtienen de la FASE 3, ACTIVIDAD ER 1, TAREA ER 1.2., misma que como se ha explicado en este capítulo, representa el resultado de las actividades y tareas previas.

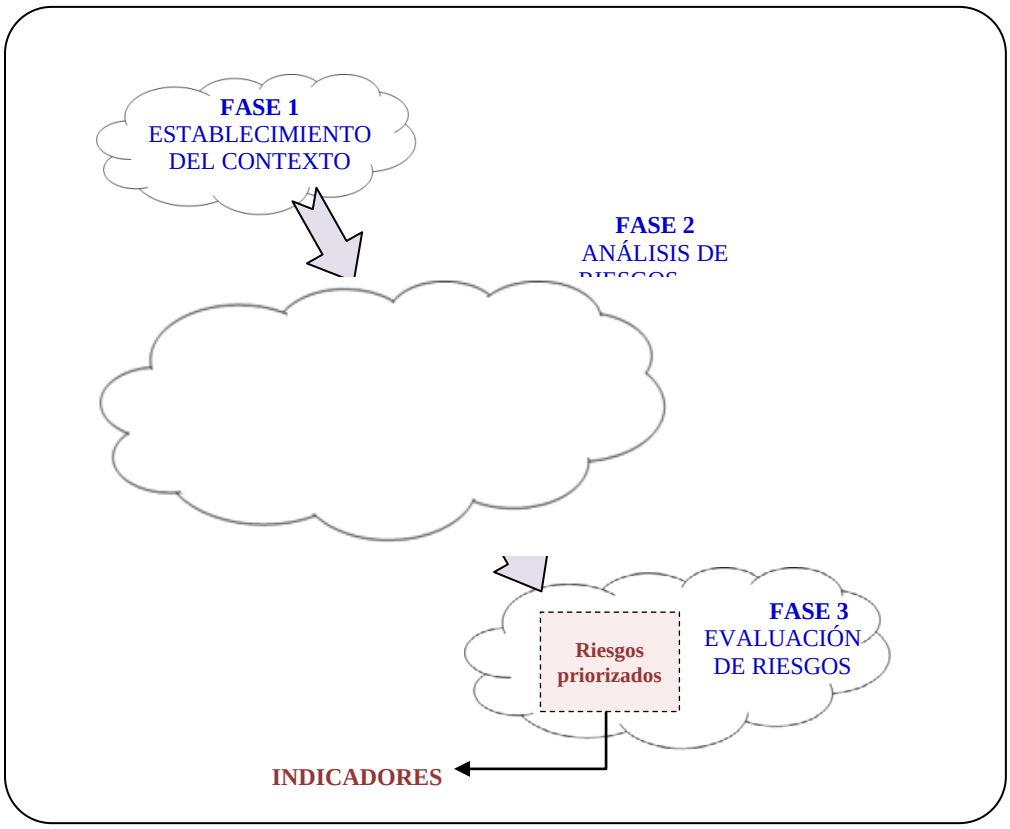


Figura 10. Esquema de obtención de indicadores.

Por lo tanto la LISTA DE RIESGOS PRIORIZADOS corresponde a los indicadores que le permiten a una empresa identificar los aspectos en los cuales debe implementar controles para minimizar dichos riesgos tecnológicos.

Es importante resaltar y revisar en este punto que como se observa de la propuesta metodológica planteada, los riesgos que constan en LISTA DE RIESGOS PRIORIZADOS provienen de la PROBABILIDAD e IMPACTO que se valoran en función de los controles que la empresa tenga inicialmente implementados.

Por lo tanto, considerando que un riesgo residual por definición, es aquél que permanece después de que una empresa desarrolla sus acciones a los riesgos (controles), se colige que la LISTA DE RIESGOS PRIORIZADOS corresponde a riesgos de este tipo y que se denominarán para referencias futuras como **riesgos residuales actuales** (previos a cualquier implantación o acción recomendada)**.**

Por su parte, los riesgos que permanecen aún después de las recomendaciones y controles que se deriven de la aplicación de la presente propuesta metodológica, corresponden a riesgos residuales que se denominarán **riesgos residuales netos.**

Entonces bajo esas premisas, la situación se explica indicando que una vez que la empresa haya implementado los controles y recomendaciones que se derivaron del proceso de gestión de riesgos, la valoración de los ***riesgos residuales netos*** resultará inferior a la valoración de los ***riesgos residuales actuales***, verificándose entonces una minimización de riesgos, todo a partir de la LISTA DE RIESGOS PRIORIZADOS:

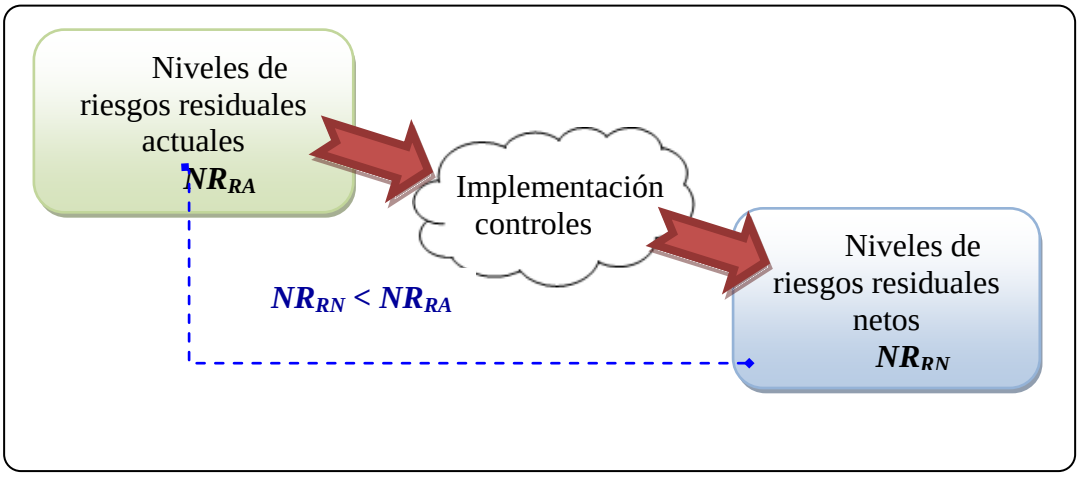


Figura 11. Niveles de Riesgo Residuales (implementación de controles).

Sin embargo, como se explica en el primer capítulo del presente estudio, la implementación de los controles recomendados escapa al alcance de esta tesis por tratarse de una decisión directa y exclusiva de la empresa ISP que decida aplicar la presente propuesta metodológica para la gestión de sus riesgos.

4.5.2.1. Estimación

Debido a que la implementación de los controles recomendados no es tema de esta tesis, para la tarea de ***estimar*** los niveles de riesgos residuales netos se considerará un procedimiento basado en la efectividad de los controles que se recomienden tras la aplicación de la propuesta metodológica planteada. Es decir:

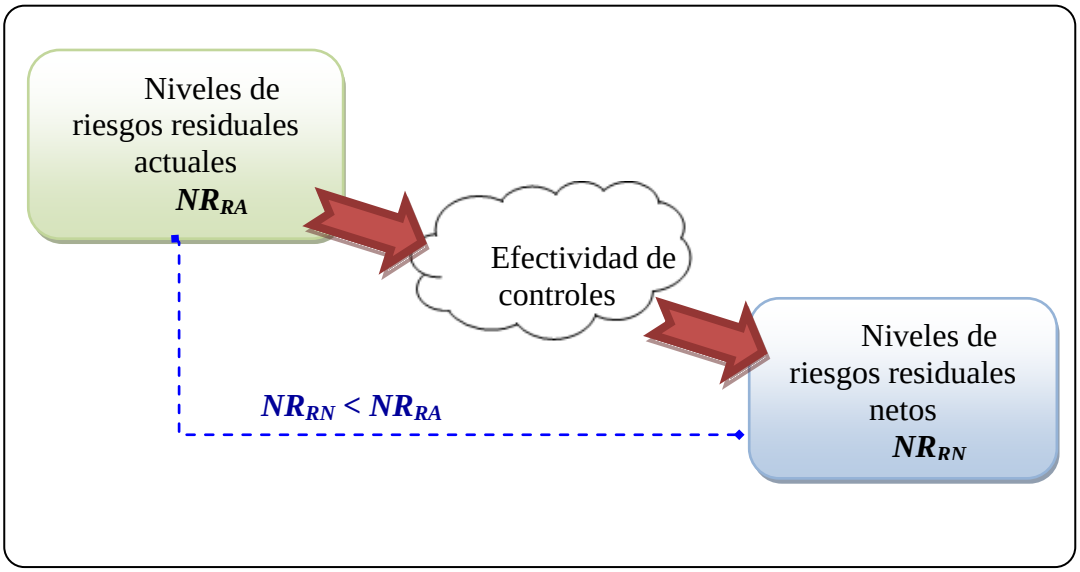


Figura 12. Niveles de Riesgo Residuales (efectividad de controles).

Por tanto, a continuación se detallan los procedimientos y criterios a considerar para estimar tanto la efectividad de los controles recomendados; así como los Niveles de Riesgos Residuales Netos (NR_{RN}).

Efectividad de los controles.- Para este caso en particular, considerando los escenarios de evaluación cualitativa utilizados para las valoraciones de PROBABILIDAD e IMPACTO, la estimación de la efectividad de los controles recomendados se ejecutará también en un modelo cualitativo, fundamentado en la descripción específica de un rango de situaciones o escenarios de control los cuales tienen una "calificación" asociada. Es decir, que las características de uno o varios controles se comparan con un conjunto definido y objetivo de alternativas.

La calificación de la efectividad de los controles se basará en dos aspectos. El principal de ellos el *nivel de automatización*:

Al respecto, a partir de la investigación de varias fuentes, se desprende por definición que la efectividad de un control se encuentra estrechamente relacionada con su fiabilidad. Por ejemplo, en ese sentido, *la Sindicatura de Comptes de la Comunitat Valenciana, en su Manual de Fiscalización Sección 315.3: Guía de*

aplicación: El conocimiento requerido del control interno de la entidad, define que los elementos manuales en tareas de control pueden resultar menos fiables que los elementos automatizados. Esto debido a que los controles manuales podrían ser más fácilmente evitados, ignorados o eludidos y también a que existe mayor exposición a simples errores y equivocaciones; y por lo tanto, no existe la garantía de que un elemento del control manual será aplicado de manera precisa y congruente.

Por su parte, un elemento automatizado (en un ambiente de TI) agrega efectividad al control, pues de manera general, permite el procesamiento de grandes volúmenes de transacciones o de datos; mejorando la disponibilidad y exactitud de la información; así como la capacidad de hacer un seguimiento de resultados, actividades, políticas, procedimientos; entre otras.

Entonces, por definición, un control automatizado alcanza mejores niveles de efectividad que un control de características manuales.

Por otra parte, otro de los aspectos que se considerarán en la estimación de la efectividad de los controles es su *naturaleza:*

- Preventivos: Son más rentables. Evitan costos de corrección. Evitan problemas antes de que aparezcan, es decir, previenen la ocurrencia de un error, omisión o ataque.

- Detectivos: Diseñados para tareas de conciliaciones, confirmación de datos, conteos, análisis de variaciones, entre otras. En general, son más costosos que los preventivos, pues no logran evitar que la amenaza se materialice.

- Correctivos: Referidos principalmente a acciones y procedimientos de rectificación que comprenden tareas de corrección generalmente desde la documentación hasta la reformulación o solución. Por tanto, en teoría resultan los más costosos de ejecutar.

Así, en consideración de los antecedentes expuestos (nivel de automatización y naturaleza de los controles) la estimación de la efectividad de los controles para esta propuesta metodológica corresponde al siguiente criterio:

$$[1] \quad \boldsymbol{Ef = PNa + PNc}$$

Donde,

Ef: Efectividad de control.

PNa: Ponderación nivel de automatización.

PNc: Ponderación naturaleza del control.

Donde además, las ponderaciones que se utilizarán para cada tipo de control son:

Tabla 35

Ponderaciones para estimación de la efectividad de controles.

AUTOMATIZACIÓN	
NIVEL	**PONDERACIÓN**
Automatizado	**2**
Manual	**1**

NATURALEZA	
NIVEL	**PONDERACIÓN**
Preventivo	**2**
Detectivo / Correctivo	**1**

Es decir, en la práctica, para cada control evaluado se aplicará el criterio *[1]* con los valores de ponderación establecidos. Por ejemplo; un control que sea de tipo

"automatizado" (ponderación: 2) y además de naturaleza "preventiva" (ponderación: 2), le corresponde una equivalencia de efectividad de nivel: 4.

Con el criterio de cálculo y las ponderaciones definidas, las escalas resultantes para la estimación de la efectividad de controles guardan relación con aquellas utilizadas en la presente propuesta metodológica para la valoración de Probabilidad, Impacto y de Riesgos.

Tabla 36

Niveles de efectividad de controles recomendados.

Niveles de efectividad de controles recomendados

Nivel	Escala
Alto	**4**
Medio	**3**
Bajo	**2**
Inexistente	**1**

Nivel de riesgo residual neto.- Varias publicaciones, entre ellas citando al denominado "SIGWEB, EL PORTAL DE LOS EXPERTOS EN PREVENCIÓN DE RIESGOS DE CHILE (http://www.sigweb.cl)" en su artículo "Matriz de Riesgo, Evaluación y Gestión de Riesgos" define al nivel de riesgo residual como la relación entre "el grado de manifestación de los riesgos inherentes y la gestión de mitigación de riesgos establecida por la administración". Trasladando dicho concepto para este caso particular, el Nivel de Riesgo Residual Neto *(NR_{RN})* corresponde entonces a la relación entre el Nivel de Riesgo Residual Actual *(NR_{RA})* y la Gestión de mitigación de riesgos (representada esta última por la efectividad del control, *Ef*):

[2] $$\boldsymbol{NR_{RN} = NR_{RA} / Ef}$$

Donde la presente propuesta metodológica define:

- Cuatro Niveles de Riesgo Residual Actual (NR_{RA}):

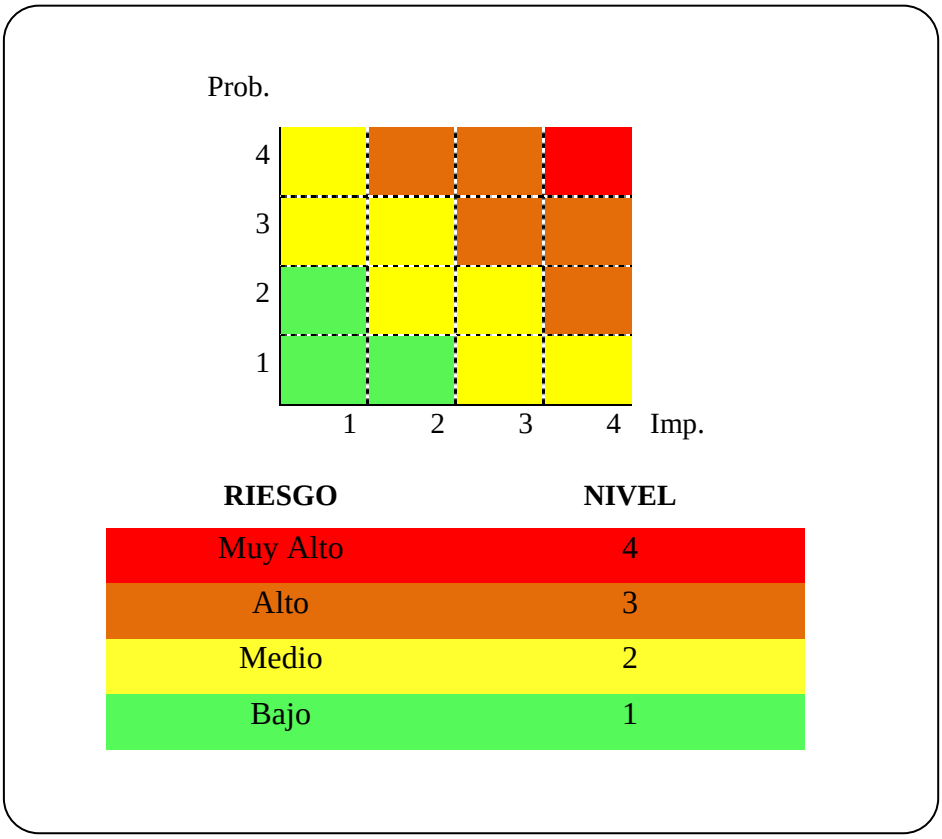


Figura 13. Niveles de Riesgo Residual Actual (NR_{RA})

- Y, cuatro niveles de efectividad de los controles recomendados que representan la gestión de mitigación de riesgos. (Tabla 36)

A partir del criterio *[2]*, se destaca que los Niveles de Riesgo Residual Neto $\boldsymbol{NR_{RN}}$ resultan menores que los Niveles de Riesgo Residual Actual $\boldsymbol{NR_{RA}}$ conforme se incrementa la efectividad de los controles recomendados $\boldsymbol{Ef}$.

4.5.3. Conclusión sobre la hipótesis.

La propuesta metodológica para la gestión de riesgos tecnológicos permite a las empresas proveedoras de Internet (ISP) contar con indicadores sobre los cuales tomar decisiones de control.

Dichas decisiones de control permiten a cada una de las empresas minimizar sus riesgos tecnológicos, toda vez que los niveles de riesgos residuales netos resultan menores a los niveles de riesgos residuales actuales.

La aplicación puntual de esta propuesta metodológica, sobre una empresa tomada como caso de estudio, se presenta en el siguiente capítulo.

CAPITULO V

APLICACIÓN DE LA PROPUESTA METODOLÓGICA PARA GESTIÓN DE RIESGOS TECNOLÓGICOS

5.1. Introducción

La propuesta metodológica para gestión de riesgos tecnológicos dentro de las empresas de telecomunicaciones ha sido implementada en una empresa de la ciudad de Quito con el objetivo de validar los resultados con información real utilizada en cada fase.

La empresa en la cual se llevó a cabo la implementación del proyecto mantiene sus políticas de confidencialidad de la información por lo cual no se revela el nombre de la misma, de igual manera los nombres de los responsables que participaron dentro del proyecto tampoco son revelados.

5.2. Aplicación

5.2.1. FASE 1. Establecimiento del contexto

5.2.1.1. ACTIVIDAD EC1: Planificación

- **TAREA EC1.1: Información y situación de la empresa**

La empresa seleccionada para la aplicación de la metodología desarrollada corresponde a un ISP de la ciudad de Quito, dedicado por tanto a la provisión de servicios de Internet a clientes estrictamente corporativos; así como al diseño, ejecución y asesoría en proyectos de telecomunicaciones.

Este ISP que en adelante se denominará “LA EMPRESA” o “CASO DE ESTUDIO” (a efecto de salvaguardar la confidencialidad y anonimato requerido por los principales de dicha organización) es una empresa orientada a brindar soluciones en todos los campos de las comunicaciones y conectividad de redes. Brinda servicios de Routing, banda ancha en transmisión de datos, banda ancha Internet, voz y video sobre IP, servicios de valor agregado, entre otros.

En general, oferta soluciones integrales en telecomunicaciones; incluyendo los servicios de instalación, mantenimiento y desarrollo de proyectos; además de asesoría tecnológica para la venta e instalación de equipos de última generación.

LA EMPRESA cuenta con su sede principal en la ciudad de Quito y mantiene presencia también en las ciudades de Guayaquil, Ibarra, Cuenca, Ambato, Latacunga y Esmeraldas.

Por otra parte, en lo que corresponde a la explotación de servicios de Valor Agregado Internet, se debe indicar que el Título Habilitante pertinente otorgado por la Secretaría Nacional de Telecomunicaciones SENATEL le autoriza a la organización a proveer servicios de Internet en la ciudad de Quito. Dicho Título fue debidamente renovado y se encuentra vigente desde el mes de mayo de 2014 hasta mayo del 2024; periodo a partir del cual la empresa deberá solicitar la debida renovación o prórroga de su permiso de operación conforme el procedimiento establecido en la normativa vigente.

Finalmente es necesario destacar que por sus iniciativas, en el año 2005 LA EMPRESA en referencia se hizo acreedora a la distinción “WORLD LEADER BUSINESS ENTERPRISE” que otorga el WORLD CONFEDERATION OF BUSINESSES para reconocer, resaltar y condecorar a las Empresas, Organizaciones y/o Personalidades líderes de cada país miembro.

a) Cultura Organizacional

La cultura organizacional está basada en sus principios empresariales constituidos por su Misión y Visión, mismas que se presentan a continuación:

- Misión.- “Nuestra experiencia, profesionalismo y capacitación permanente, nos permiten brindar asesoría de calidad en el diseño, ejecución de proyectos de telecomunicaciones y servicios de internet, encaminados a encontrar la mejor solución técnico-económica para satisfacer las necesidades de nuestros clientes.”.

- Visión.- "Ser el mejor proveedor en servicios de telecomunicaciones, internet y equipamiento a nivel nacional con proyección internacional. Corporativamente sólidos y con nuestras alianzas estratégicas comerciales, estaremos en capacidad de ofrecer a nuestros clientes, las mejores soluciones en comunicaciones con tecnología de punta a los precios más competitivos del mercado.".

- Valores:

- Calidad Compromiso.
- Cumplimiento.
- Liderazgo.
- Confiabilidad.
- Respeto.
- Trabajo en equipo.

- Servicios

- Asesoría en telecomunicaciones.
- Desarrollo de proyectos personalizados en telecomunicaciones:
    - Instalación.
    - Mantenimiento.
    - Venta de equipos.
- Servicio de Valor Agregado, modalidad Internet.
    - Internet Banda Ancha – Home (planes residenciales).
- Servicios de red.
    - Routing y Switching.
    - Voz y video sobre IP.
    - Cableado estructurado.

Estos servicios son proporcionados por la organización en las ciudades de Quito, Guayaquil, Ibarra, Cuenca, Ambato, Latacunga y Esmeraldas; orientándose siempre hacia clientes de tipo corporativo. Es así que, entre ellos, figuran importantes instituciones (tales como agencias bancarias de amplia presencia nacional) que requieren elevada disponibilidad y calidad de servicios.

Por su parte, como se explicó anteriormente, el Servicio de Valor Agregado, modalidad Internet: Internet Banda Ancha, es provisto únicamente en la ciudad Quito en virtud del área geográfica de cobertura autorizada en su permiso de operación.

b) Involucrados y sus expectativas respecto de la empresa.

Clientes

Servicio de calidad con oportunidad.

Accionistas

Rentabilidad

Imagen corporativa

Empleados

Estabilidad

Buen ambiente laboral

Justa remuneraciones

Proveedores

Seriedad

Fidelidad

Equipo directivo

Cumplimiento de objetivos

Gobierno

Cumplimiento de obligaciones tributarias y técnicas.

Transparencia

Sociedad

Responsabilidad social

Generación de empleo

c) Regulaciones

LA EMPRESA del caso de estudio fue constituida bajo las leyes y políticas del Estado ecuatoriano, regida por la *Ley de Compañías* y siendo por lo tanto la Superintendencia de Compañías su órgano rector.

Para el cumplimiento de sus obligaciones financieras, la empresa cumple además con las denominadas Normas Internaciones de Información Financiera – NIIF adoptadas por la Superintendencia de Compañías para todas las organizaciones y entes sujetos al control y vigilancia.

En lo que al ramo de telecomunicaciones se refiere, en cuanto a la provisión del Servicio de Valor Agregado, modalidad Internet, la empresa está sometida a la Ley Especial de Telecomunicaciones y su Reglamento General; siendo regulada por el Consejo Nacional de Telecomunicaciones CONATEL; y, técnicamente controlada por la Superintendencia de Telecomunicaciones SUPERTEL.

Por su condición de proveedor de Internet, la empresa se debe además al Reglamento para la prestación de Servicios de Valor Agregado (Resolución 534-22-CONATEL-2006), a la Norma de Calidad para la prestación de Servicios de Valor Agregado (Resolución 216-09-CONATEL-2009), al Reglamento para los Abonados/Clientes-Usuarios de los servicios de Telecomunicaciones y de Valor Agregado (Resolución TEL-477-16-CONATEL-2012) y a los términos y condiciones establecidas en su título habilitante: “Permiso para la explotación de servicios de Valor Agregado, modalidad Internet”.

d) Políticas.

Políticas de calidad.- Dedicada a proveer servicios de telecomunicaciones, internet y comercializar equipos de computación. Su política de calidad está orientada por lo tanto a la satisfacción de sus clientes mediante la mejora continua en su Sistema de Gestión de la Calidad a través de controles en los procesos internos, incrementando las ventas, optimizando las compras y manteniendo la liquidez de la empresa.

La comunicación de la política de calidad se realiza a través de:

- Manual del sistema de gestión de calidad.
- Charlas planificadas para difundir al personal.
- Publicar las políticas y los objetivos en sitios visibles de la organización.

- En la inducción al personal nuevo.

Política de comunicación interna.- La práctica efectiva de esta política requiere ser contemplada de forma estructural, entre las políticas y las estrategias de la Empresa, por lo que en el procesos de implantación deben estar implicados los máximos responsables de la empresa ya que es preciso incorporar a la gestión procedimientos, normativas, circuitos, mecanismos e instrumentos que aseguren la circulación de la comunicación como un flujo estable que lubrica permanentemente toda la organización.

- El principal medio de comunicación dentro de la organización, serán las reuniones semanales, periódicas de planificación de actividades de cada Área.
- Los jefes de departamento informarán sobre los planes del Departamento e interactuarán con los empleados para establecer el dialogo.
- El empleado puede presentar varias dudas o preguntas sobre temas específicos.
- Comunicar vía mail al personal que sea necesario.
- Existirán reuniones semanales, periódicas entre los Jefes Departamentales con el objetivo de canalizar y sincronizar las tareas dependientes de los diferentes Departamentos.
- Los archivos comunes de interés para la realización de las tareas de los empleados, estarán disponibles en la red con los accesos y seguridades pertinentes.
- Las comunicaciones generales podrán ser evidenciadas en la cartelera general.
- Los jefes Departamentales y Gerentes podrán enviar memorándums a los empleados, los mismos que deben ser canalizados con responsabilidad por parte de los empleados.

Política de seguridad de la información.- Los activos de información y los equipos informáticos son de vital importancia para la empresa, sin ellos la organización quedaría rápidamente fuera de operación. Por tal razón la Gerencia y la

Junta Directiva tienen el deber de preservar, utilizarlos y mejorarlos. Esto significa que se deben tomar acciones apropiadas para asegurar que la información y los equipos informáticos estén apropiadamente protegidos.

Las distintas gerencias de la Compañía están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de la información estén suficientemente protegidos. A continuación se detallan las responsabilidades:

- La Gerencia de Tecnología es responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la junta directiva.
- Evaluar, adquirir e implantar productos de seguridad informática y realizar las demás actividades necesarias para garantizar un ambiente informático seguro.
- Proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.
- El administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra.
- El Administrador de Sistemas es responsable de informar al Jefe de Seguridad (Supervisor Técnico) y a sus superiores sobre toda actividad sospechosa o evento insólito.

Los usuarios son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

- No divulgar información confidencial de la Compañía a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.
- No utilizar los recursos informáticos y de telecomunicaciones para otras actividades que no esté directamente relacionados con el trabajo en la Compañía.
- Proteger meticulosamente su contraseña y evitar que sea visto por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato o al Administrador de sistemas cualquier evento que puede comprometer la seguridad de la Compañía y sus recursos informáticos. (virus, pérdida de datos, etc.).

Política de seguridad para computadores.

- Los equipos de computación deben usarse en ambientes seguros, es decir implantar las medidas de control necesarias para proteger el software, hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
- Solo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Deben respetarse y no modificar la configuración de hardware y software establecida por el administrador de Informática.
- No se permite fumar ni comer o beber mientras se está usando un PC.
- Deben protegerse los equipos de riesgos de medioambiente (polvo, incendio, agua, etc.).
- Debe usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder no interrumpibles (UPS).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como perdida de la información o indisponibilidad de los servicios.

- Los equipos deben marcarse para su identificación y control de inventario. Lo registros de inventario deben mantenerse actualizados.
- No pueden moverse los equipos o reubicarse sin permiso y para llevar un equipo fuera de la compañía se requiere una autorización escrita.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad requiriendo una contraseña al reasumir la actividad.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando pierdan su utilidad, los datos confidenciales deben ser borrados.
- Debe implantarse un sistema de autorización y control de acceso, con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar o borrar datos de importancia para la Compañía.
- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red local.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Compañía está protegido por derechos de autor y requiere licencia de uso, por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- Los usuarios no deben copiar a un medio removible (pendrive usb), el software a información residentes en las computadoras de la Compañía sin una aprobación previa por la Gerencia o del administrador de Sistemas.
- No pueden extraerse información fuera de la sede de la Compañía sin la previa autorización por Gerencia. Esta política es particularmente pertinente a aquellos que usan computadores portátiles o están con acceso a internet.

- Debe instalarse una herramienta antivirus, la cual debe mantenerse actualizada. Notificar a seguridad informática la presencia de virus.
- Solo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Compañía.
- No debe usarse software descargado de la web (internet) sobretodo que provenga de una fuente no confiable, a menos que este comprobado de forma rigurosa y sea aprobado su uso por el departamento de sistemas.
- Para prevenir demandas legales o la introducción de virus, se prohíbe estrictamente la instalación de software no autorizado, así mismo no se permite el uso de software de distribución o shareware, a menos que haya sido aprobado por el departamento de Sistemas.
- Para ayudar a restaurar los programas originales, deben hacerse copias de todo software nuevo antes de su uso y deben guardarse en un lugar seguro. Esto será responsabilidad del Jefe de Seguridad en coordinación con el administrador de los Sistemas.
- No deben usarse medios de almacenamiento en cualquier computador de la Compañía a menos que haya previamente verificado que estén libre de virus u otros agentes dañinos.
- Periódicamente deben hacerse respaldos de información que el Jefe de Seguridad reconozca como importante, dichas copias deben guardarse en un lugar seguro a prueba de hurto, incendio e inundaciones. Los datos e información vitales para la operación de la Compañía debe guardarse en otra sede, lejos del edificio, lugar definido por el Jefe de Seguridad.
- Los usuarios de PCs son responsables de proteger los programas y datos contra perdida o daño. Para sistemas multiusuario y de comunicación, el Administrador de cada uno de estos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo. Esta tarea periódica deberá ser cumplida de forma obligatoria por los usuarios y por el Administrador de la Red.

- La información de la Compañía clasificada como confidencial o de uso restringido, debe guardarse con los password de acceso.
- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.
- Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que se les mande a reparar. De no ser así la reparación debe ser efectuada por empresas responsables con las que se haya firmado un contrato de confidencialidad. Alternativamente la reparación de efectuarse bajo la supervisión de un representante de la Compañía.
- El personal que utiliza un computador portátil que contenga información confidencial de la Compañía, no debe dejarla desatendida, sobre todo cuando este de viaje y ademán esa información debe estar cifrada.

Políticas de seguridad para las comunicaciones (teléfono, e-mail, fax)

Propiedad de la Información.- La Compañía promueve el uso responsable de las comunicaciones en forma electrónica, en particular e teléfono, correo de voz, e-mail. Los sistemas de comunicación y los mensajes generados y procesados, incluyendo las copias de respaldo, se deben considerar como propiedad de la Compañía y no de los usuarios de los servicios.

Uso de los sistemas de comunicación.- Los sistemas de comunicación de la Compañía generalmente deben usarse para actividades de trabajo. El uso personal en forma ocasional siempre y cuando consuma una cantidad mínima de tiempo y recursos y no interfiera con la productividad.

Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

El e-mail será el canal de comunicación general de la Compañía, toda comunicación importante deberá ser enviada por este medio y el usuario mantendrá por un periodo considerable de tiempo una copia de esta información.

Siendo el e-mail un documento importante, cada usuario deberá en coordinación con el Administrador de la Red guardar la información pertinente en un respaldo en el mismo PC o donde el Administrador pueda guardar información de usuarios.

La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse las horas no laborables.

Confidencialidad y privacidad.- Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades pero también introducen nuevos riesgos. No deben enviarse a través de internet mensajes con información confidencial a menos que esté cifrada.

Los empleados y funcionarios de la Compañía no deben interceptar las comunicaciones o divulgar su contenido. La Compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto ocasionalmente es necesario interceptar ciertas comunicaciones.

Reenvío de mensajes.- Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Compañía, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Compañía sin la debida aprobación.

Borrado de mensajes.- Los mensajes que ya no se necesiten deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información.

Políticas de seguridad para redes.

El propósito de esta política es establecer directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Compañía al estar conectada a redes de computadoras. Esta política aplica a todos los empleados, contratistas, consultores y personal temporal de la Compañía.

Es política de la Compañía prohibir la divulgación, duplicación, modificación, destrucción, perdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Modificaciones

Todos los cambios en la central telefónica (PBX) y en los servidores y equipos de red de la Compañía, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switches, deben se documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios.

- Al recibir una nueva cuenta, el usuario debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad y acepta sus responsabilidades con relación al uso de esa cuenta.
- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente probada por el Administrador.
- No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, solo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior y en particular cuando un empleado cesa en sus funciones.
- Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.
- Contraseñas y control de acceso.
- El usuario no debe guardar su contraseña en una forma legible en archivos, en discos, ni escribir en papel. Si hay razón para creer que una contraseña ha sido comprometida, de cambiarla inmediatamente.
- No usar contraseñas idénticas al nombre de usuario o similares a contraseñas anteriores.
- Nunca debe compartirse la contraseña o revelarla a otros.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos o aplicaciones.
- La contraseña inicial emitida a un nuevo usuario solo debe ser válida para la primera sesión.
- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switches, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a tres el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema.
- Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda uso de un sistema de autenticación más robusto.
- Si no hay actividad en un terminal, PC o estación de trabajo durante un periodo establecido, el sistema debe suspender la sesión.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones que serian la causa para un despido.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro que involucre a los sistemas informáticos.
- Los archivos de bitácora logs y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses.
- Los servidores de red y los equipos de comunicación deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas.

Ambiente interno

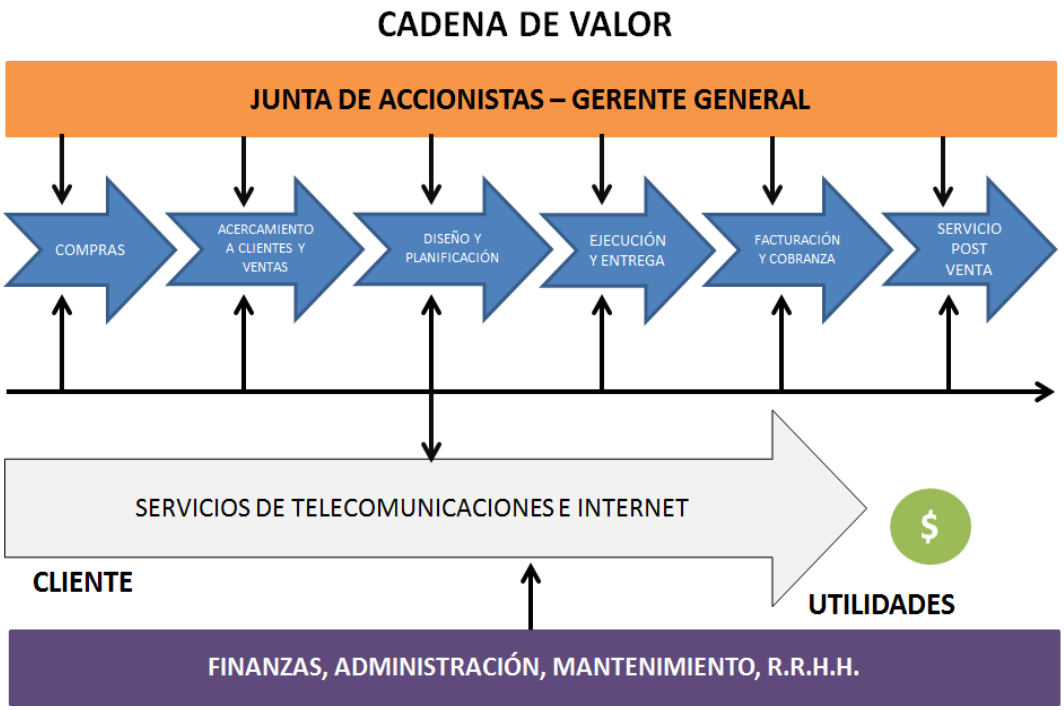


Figura 14. Cadena de Valor de la empresa del caso de estudio.

Fuente: Información proporcionada por la empresa del caso de estudio.

Mapa de Procesos

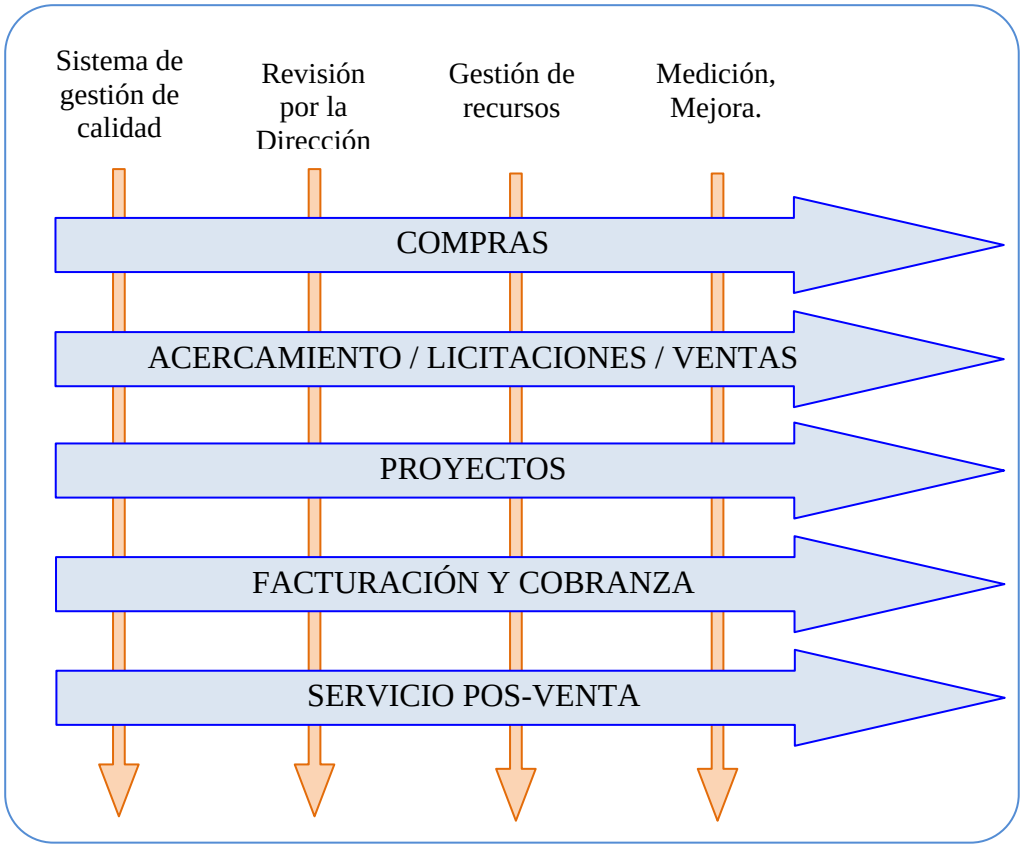


Figura 15. Mapa de Procesos de la empresa del caso de estudio.

Fuente: Información proporcionada por la empresa del caso de estudio.

- **TAREA EC1.2 Determinación del alcance**

En base a la información recopilada se plantea el alcance que tendrá la evaluación de riesgos tecnológicos; con el propósito de enfocar el análisis en los recursos críticos de la organización y lograr los objetivos definidos en la propuesta metodológica en estudio. Por tanto, el proceso involucrará directamente al área de tecnología, específicamente a:

- La Gerencia del Departamento de tecnología.
- Los coordinadores y operadores que forman parte del Departamento de tecnología.
- Activos intangibles

  - Información y datos: resaltar la importancia de la información dentro del negocio para establecer una clasificación.
  - Políticas: considerar las políticas de la empresa en lo referente al manejo de información y seguridad, principalmente.
  - Procesos del negocio: considerar los procesos críticos del negocio que pudiera ser o no automatizados mediante la tecnología implementada en la Empresa.

- Activos tangibles.
  - La infraestructura tecnológica: Hardware y Software.
  - Sistemas de red.

- Recurso humano que hace uso de la tecnología disponible en la empresa

Sobre esa base, el alcance que tendrá la propuesta metodológica al ensayarse sobre la empresa, será en general:

- Ejecutar la evaluación y valoración de riesgos para los activos tecnológicos de la empresa; y,
- Definir las recomendaciones necesarias para el tratamiento de los riesgos de la empresa.

- **TAREA EC1.3 Plan de Trabajo en la empresa del caso de estudio.**

El plan de trabajo define el calendario de cumplimiento de las distintas etapas, actividades y tareas del proyecto de gestión de riesgos que se aplica en la empresa del caso de estudio.

Debido a que para el desarrollo del proyecto se requiere considerar la disponibilidad de recursos (técnicos, administrativos, humanos, etc.) de la empresa, dicho plan de trabajo se define a través de una continua comunicación e interacción con los responsables de cada proceso. El plan de trabajo establecido se muestra en el Anexo 5.

5.2.1.2. ACTIVIDAD EC2: Aprobación

- **TAREA EC2.1. Aprobación por el Departamento de Tecnología.**

Se realiza el acta para la reunión con el departamento de Tecnología con el propósito de obtener la aprobación del plan de trabajo a efectuarse.

Tabla 37

Ejemplo de acta de reunión utilizada

ACTA DE REUNIÓN		
ACTA N°: **2** FECHA:	**HORA INICIO:** **HORA FINAL:**	**LUGAR:** Sala de reuniones de la Empresa
OBJETIVO DE LA REUNIÓN. Presentación del proyecto y aprobación por parte del departamento tecnológico o de seguridad de la información.		
RESPONSABLES DE LA REUNIÓN. - ING. NELSON MONTEROS - ING. RUBÉN FERNÁNDEZ		
CONVOCADOS / ASISTENTES		
XXXXXXXXX		GERENTE DE TECNOLOGÍA
TEMAS TRATADOS: - Se plantea el alcance de la metodología en base a la información recopilada con el propósito de enfocar el análisis en los recursos críticos de la organización sin extenderse a recursos irrelevantes. - Se presenta el cronograma de trabajo a desarrollarse por parte de los promotores del proyecto, el cual es revisado en base a recursos y tiempo de ejecución de cada fase. - La gerencia de tecnología una vez revisado el cronograma, aprueba y concede la definición de recursos y tiempos requeridos por parte de los responsables del proyecto.		
FIRMAS DE LOS PARTICIPANTES: Ing. Nelson Monteros Gerente de Tecnología		Ing. Rubén Fernández

- **TAREA EC2.2. Aprobación de la Gerencia.**

Con el visto bueno de la Gerencia de Tecnología, se requiere la aprobación final por parte de la gerencia general para dar inicio a la ejecución del proyecto de Gestión de Riesgos Tecnológicos.

Tabla 38

Ejemplo de acta de reunión utilizada

ACTA DE REUNIÓN			
ACTA N°: **2**	**HORA INICIO:**	**LUGAR:**	Gerencia
FECHA:	**HORA FINAL:**	General	

OBJETIVO DE LA REUNIÓN.

Solicitar la aprobación del plan de trabajo para la Gestión de Riesgos por parte de la Gerencia General.

RESPONSABLES DE LA REUNIÓN.

- ING. NELSON MONTEROS
- ING. RUBÉN FERNÁNDEZ

CONVOCADOS / ASISTENTES

XXXXXXXXX	GERENTE GENERAL
XXXXXXXXX	GERENTE DE TECNOLOGÍA

TEMAS TRATADOS:

- Se presenta la solicitud de aprobación para el desarrollo del proyecto, en el cual se especifica el alcance del proyecto junto con el cronograma de trabajo, adjunto el visto bueno del departamento de Tecnología.
- Con el respectivo sello y firma la empresa aprueba y respalda la ejecución del proyecto.

FIRMAS DE LOS PARTICIPANTES:

Ing. Nelson Monteros	Ing. Rubén Fernández
Gerente General	Gerente de Tecnología

5.2.1.3. ACTIVIDAD EC3: Comunicación del proyecto.

- **TAREA EC3.1 Presentación y comunicación del proyecto.**

A continuación se emite un memorando dirigido a los involucrados a colaborar en el proyecto, el mismo es despachado por la Gerencia General.

Tabla 39

Tarea para comunicación del proyecto (Ejemplo Memorando utilizado).

MEMORANDO

DE: **Gerente General**

CC: **Responsables del Proyecto**

PARA: **Involucrados**

ASUNTO: **Ejecución del Proyecto Gestión de riesgos Tecnológicos dentro de la Empresa.**

FECHA:

Debido a la gran dependencia de las tecnologías dentro del negocio de la empresa, el departamento de Tecnología llevara a cabo la ejecución del proyecto GESTIÓN DE RIESGOS TECNOLÓGICOS, por lo que solicito a los involucrados colaborar en el levantamiento de la información que requieran los responsables del proyecto.

El objetivo del proyecto servirá para conocer el nivel de riesgos a los que se encuentra sometida la empresa, lo que permitirá tomar las medidas de protección necesarias para los intereses de la empresa.

Atentamente,

Gerente General

5.2.2. FASE 2. Análisis de riesgos

5.2.2.1. ACTIVIDAD AR1: Identificación de Riesgos

- **TAREA AR1.1. Identificación de activos.**

Se levanta el inventario de activos tecnológicos que se encuentran relacionados directamente con los procesos del negocio, organizados en las categorías propuestas por la metodología, es decir:

- Activos primarios.
- Activos tangibles.
- Activos intangibles; y,
- Servicios IT.

Tabla 40

Listado de activos dentro de la empresa.

CLASE DE ACTIVO	TIPO
Primario	Procesos
Tangibles	Infraestructura física
	Información de interés para el negocio
	Información comercial y financiera
	Información vital
	Información personal
Intangibles	Intangibles
Servicios IT	Mensajería
	Infraestructura de Core
	Aplicaciones y Software licenciado

Para el efecto se considera como productos de entrada, la lista de activos con:

a. Propietarios (responsables).
b. Procesos en los que se involucran.
c. Función

Producto de salida:

Un inventario de los activos de la Organización.

El detalle del inventario de activos tecnológicos recopilado en la empresa del caso de estudio se presenta en el Anexo 6.

- **TAREA AR1.2. Identificación de amenazas.**

Se define un mapa o catálogo de amenazas bien identificadas, acogiéndose para el efecto como referencia y base, el inventario de mapas que propone MAGERIT V3., y se considera además otras diferentes fuentes (entrevistas, reuniones e información analizada) que permitan incluir o desestimar otras posibles amenazas para el entorno.

Productos de entrada:

- El listado de amenazas de la propuesta metodológica que se presenta toma como referencia el catálogo de amenazas establecidas por la metodología MAGERIT V3.
- Levantamiento de información, tanto dentro como fuera de la empresa, sobre incidentes reportados.
- Informes y aportes de los “propietarios de los activos”.
- Retroalimentación: Actualización de escenarios de amenazas, debido a que las mismas muchas veces son variantes de otras anteriores y pueden surgir nuevas amenazas.

Salida:

Una lista de amenazas reales, clasificadas según su tipo y origen.

Para el caso de la empresa de caso de estudio, las amenazas sobre las cuales se basa la evaluación son:

Tabla 41

Amenazas consideradas para análisis de riesgos.

AMENAZAS
I. DE ORIGEN INDUSTRIAL
Fuego
Daños por agua
Explosiones, sobrecarga eléctrica, corte del suministro eléctrico, etc.
Contaminación mecánica
Contaminación electromagnética
Avería de origen físico o lógico
Condiciones inadecuadas de temperatura
Fallo de servicios de comunicaciones
Interrupción de otros servicios y suministros esenciales
Degradación de los soportes de almacenamiento de la información
II. ERRORES Y FALLOS NO INTENCIONADOS
Errores de los usuarios
Errores del administrador
Errores de monitorización (log)
Deficiencias en la organización
Difusión de software dañino
Errores de [re-]encaminamiento
Escapes de información
Alteración accidental de la información
Destrucción de información
Fugas de información
Vulnerabilidades de los programas (software)
Errores de mantenimiento / actualización de programas (software)
Errores de mantenimiento / actualización de equipos (hardware)
Caída del sistema por agotamiento de recursos
Pérdida de equipos

Continúa →

III. ATAQUES INTENCIONADOS
Manipulación de los registros de actividad (log)
Manipulación de la configuración
Suplantación de la identidad del usuario
Abuso de privilegios de acceso
Difusión de software dañino
Alteración de secuencia
Acceso no autorizado
Repudio
Interceptación de información (escucha)
Destrucción de información
Divulgación de información
Manipulación de programas
Manipulación de los equipos
Denegación de servicio
Robo
Ataque destructivo
Extorsión
Ingeniería social (picaresca)
IV. INSTITUCIONALES
Adquisición de tecnología sin previo análisis
Personal con conocimiento desactualizado
Indisponibilidad del personal
Mal uso de Internet y otros recursos tecnológicos

Fuente: Referencia del inventario de amenazas de MAGERIT V3.

- **TAREA AR1.3. Identificación de Controles Existentes.**

Para continuar con la ejecución del proyecto, es importante reconocer los controles existentes en base a las amenazas identificadas que podrían materializarse y afectar a la organización. Así mismo éstos deben ser clasificados según su "Naturaleza" en: preventivos, detectivos y/o correctivos.

Esta información se obtiene dentro de la empresa tomando las diferentes fuentes y personal involucrado.

Productos de Entrada:

- Mapa de amenazas.
- Políticas, procedimientos, estructuras de control.
- Planes de tratamiento de riesgos implementados.
- Evaluaciones de control interno y su implementación (de existir)

Acción:

Efectuar un levantamiento de los controles implementados para combatir las amenazas de la organización.

Es fundamental identificar a los funcionarios responsables tanto de la ejecución como de la validación del cumplimiento de los controles, esta tarea se realiza como parte del proceso de entrevistas en donde los principales involucrados son el personal del Área de Informática, Seguridad Informática y personal de evaluación de riesgos.

Salida:

Un escenario de los controles existentes, planificados, su grado de implementación, uso y efectividad.

Los controles existentes en la empresa del caso de estudio, se detallan en el Anexo 7.

- **TAREA AR1.4. Identificación de Vulnerabilidades**

Luego de haber mantenido las debidas reuniones con el personal involucrado para obtener los controles existentes, junto con las amenazas identificadas y alguna información adicional, el objetivo de este punto es detectar las vulnerabilidades que se encuentran dentro de la organización.

Productos de Entrada:

- Informes internos de vulnerabilidades (de existir).
- Listas de vulnerabilidades conocidas.
- Reportes de incidentes.

- Inventario de activos.

Acción:

- Las vulnerabilidades tienen su importancia relativa en función de la existencia de amenazas reales, que puedan explotarla, y el impacto que eso pueda generar para la Organización.
- Se consideran los controles existentes (y planificados) que pueden mitigar o eliminar dicha vulnerabilidad.
- Si se detectan vulnerabilidades que no tienen una amenaza conocida, debe documentarse, porque el escenario y las amenazas podrían cambiar.

Salida:

Una lista de vulnerabilidades de los activos, considerando las amenazas y controles existentes y las Vulnerabilidades sin relación con amenazas identificadas inicialmente.

El listado de las vulnerabilidades detectadas en la empresa del caso de estudio se presenta en el Anexo 7.

5.2.2.2. ACTIVIDAD AR2: Estimación de Riesgos

- **TAREA AR 2.1. Metodología para la estimación del riesgo**

La empresa del caso de estudio, tal como se colige en la aplicación de la Fase 1: Establecimiento del contexto; y Fase 2: Análisis de riesgos, no cuenta con información que derive de una evaluación de riesgos previa. Además, esta empresa no posee una política formal, proceso o marco de referencia implementado para la administración y gestión de riesgos.

Ante esa situación y de la manera en que se explicó en el desarrollo de la propuesta metodológica, resulta adecuado establecer una estimación cualitativa de riesgos para la empresa del caso de estudio, aprovechando el alto grado de comprensión de dicha método.

La subjetividad a la que está sujeta por naturaleza una estimación de tipo cualitativa, se minimizará con el establecimiento de criterios de calificación que se detallan en cada una de las tareas de valoración respectivas.

- **TAREA AR 2.2. Valoración de los incidentes (Probabilidad)**

Para la estimación de probabilidad se consideran:

Productos de entrada:

- Identificación de activos
- Identificación de amenazas
- Identificación de controles existentes
- Identificación de vulnerabilidades

Acción:

Para el caso de la empresa en estudio, la estimación se efectúa a través de un método cualitativo, tal como se explica en la tarea AR 2.2. Las escalas definidas para el efecto son las que se muestran a continuación:

Tabla 42

Escalas para estimación de la probabilidad.

ESCALA	ESTADO NATURAL	VALOR	PROBABILIDAD
ALTA	**Probabilidad de ocurrencia del riesgo al no existir controles que impidan el desarrollo del incidente o ataque. La materialización de la amenaza es inminente.**	**4**	**76% - 100%**
MODERADA	**Probabilidad de ocurrencia del riesgo ante controles cuya implementación no se encuentra documentada y/o demostrada durante evaluación.**	**3**	**51% - 75%**

Continúa→

MEDIA	**Probabilidad de ocurrencia del riesgo ante controles implementados con documentación inadecuada y/o incompleta.**	**2**	**26% - 50%**
BAJA	**Probabilidad de ocurrencia del riesgo ante controles implementados y que se encuentran documentados, difundidos y/o monitoreados.**	**1**	**1% - 25 %**
NINGUNA	**No existen condiciones que impliquen riesgo.**	**0**	**0%**

Una equivalencia porcentual a cada una de las escalas de probabilidad puede relacionarse de la forma en que consta en la Tabla anterior.

Salida

Se obtiene una matriz de probabilidad estimada para cada uno de los riesgos identificados, atendiendo a las amenazas identificadas, las vulnerabilidades y los controles existentes.

Dicha matriz, para la empresa del caso de estudio, se presenta en el Anexo 7.

- **TAREA AR 2.3. Valoración de las consecuencias (Impacto)**

En ese punto se busca estimar el nivel de impacto que causaría a los diferentes activos la materialización de una amenaza, la importancia de cada activo e información que ha sido brindada por el personal de la empresa es un criterio fundamental para determinar el impacto de daño que podría ocasionar a la empresa.

Entrada:

- La identificación de los procesos de negocio (clasificados según criticidad),
- Inventario de activos por categoría.
- Las amenazas a los activos

Acción:

- Matriz que involucre las amenazas y los activos de la empresa a ser evaluados.
- Identificar el impacto sobre los activos que supondría la concreción de esas amenazas, en términos de pérdida de confidencialidad, integridad y/o disponibilidad.

Salida:

Una lista de potenciales incidentes hacia varios activos, escenario con sus impactos asociados.

La escala que se utilizará se basa en los criterios definidos en la presente propuesta metodológica para la gestión de riesgos tecnológicos, específicamente en la tarea AR 2.3 del capítulo anterior; en la cual se definen cuatro niveles de impacto sobre los cuales efectuar el análisis:

Tabla 43
Escala de estimación del Impacto (consecuencias).

ESCALA DE IMPACTO	
Catastrófico	4
Alto	3
Moderado	2
Insignificante	1
No aplica / Ninguno.	0

Los resultados de la valoración del impacto se observan en el Anexo 8.

- **TAREA AR 2.4. Estimación del nivel de riesgo (Probabilidad Vs. Impacto).**

Para el establecimiento del nivel de riesgos y su consiguiente priorización, resulta más eficiente el adoptar estrategias de evaluación cualitativas, caso que aplica a empresas medianas o grandes.

Productos de entrada.

a. Lista de consecuencias valorada (impacto).
b. Probabilidad de un escenario de incidente.

Acción

El concepto tradicional de nivel de riesgo, está dado por el impacto ponderado por la Probabilidad de ocurrencia, es decir: *Impacto x Probabilidad de Ocurrencia*. El objetivo es disponer de una calificación de riesgos a los efectos que puedan priorizarse los mismos para su tratamiento.

Salida:

Una matriz con los riesgos, calificados con su nivel correspondiente en función del criterio establecido atendiendo a su impacto estimado en el negocio y a su probabilidad de ocurrencia.

El resultado de la estimación del nivel de riesgo, con el criterio de cálculo definido para la tarea AR 2.4., se presenta en el Anexo 9.

5.2.3. FASE 3. Evaluación de riesgos

5.2.3.1. ACTIVIDAD ER 1: Evaluación y priorización de riesgos.

- **TAREA ER 1.1. Lista de riesgos priorizados.**

Se establece el nivel de riesgo combinando la probabilidad de ocurrencia por el impacto. El objetivo principal de la evaluación de riesgos es priorizar los mismos y racionalizar los recursos disponibles para la implantación de controles.

Se considera toda la información relevada y analizada. Además debe establecerse una lista prioritaria a nivel macro, de los riesgos a atender con prioridad, que resultará de los procesos y activos críticos y los riesgos que pueden ocasionarle mayor daño a la empresa y que tengan una probabilidad alta de ocurrencia.

Entrada:

a. Matriz con riesgos calificados o valorados.
b. Criterios de evaluación del riesgo.

Salida:

a. Un documento con los riesgos evaluados en las áreas críticas y de alta prioridad.
b. Una lista de riesgos eventualmente inadvertidos a alto nivel o subestimados a consideración de especialistas de un dominio específico (propietarios de la información).

La lista de riesgos priorizados se presentan en el Anexo 10.

5.2.4. FASE 4. Tratamiento de riesgos

5.2.4.1. ACTIVIDAD TR 1: Respuesta al riesgo.

- **TAREA TR 1.1. Identificar opciones de tratamiento (Recomendaciones).**

Sobre la base del análisis de riesgos efectuado a la empresa ISP del caso de estudio, a continuación se detallan las recomendaciones que le son aplicables:

- Actualizar las políticas de Seguridad de la Información contenidas en el documento “Gestión de la Calidad” de la empresa ISP; el mismo que deberá incluir al menos, su definición, objetivos y alcance; así como un marco para el establecimiento de los controles; cumplimiento de requisitos legales, regulatorios y contractuales; consecuencias de las violaciones a la política de seguridad; responsabilidades generales y específicas; comunicación de

incidencias, procedimientos para autorización de privilegios y permisos a los sistemas, entre otros.

- Actualizar las políticas de Comunicación Interna incluidas en el documento “Gestión de la Calidad” de la empresa ISP; el mismo que deberá establecer lineamientos generales destinados a coordinar la comunicación interna de la empresa y administrar los correspondientes recursos comunicacionales; incluyendo los principios que regirán dichas comunicaciones, responsables de la gestión de contenidos y de medios, tipo de información circulable, indicadores de gestión, entre otros.

- Ejecutar campañas de comunicación, concientización, entrenamiento y aplicación de las políticas establecidas en la empresa ISP; dando a conocer que su cumplimiento es de carácter obligatorio, informando además las consecuencias y sanciones correspondientes por incumplimientos e inobservancias.

- Ejecutar evaluaciones y auditorías de seguimiento al cumplimiento de las políticas institucionales de la empresa.

- Definir un esquema de clasificación de datos y de información de toda la empresa, en función de criterios de confidencialidad, integridad, sensibilidad y criticidad de la misma. Dicho esquema deberá ser insumo y considerando dentro de las políticas de Comunicación Interna y de Seguridad de la Información.

- Desarrollar un plan de continuidad del negocio, inicialmente sobre la base de las principales amenazas detectadas para la empresa ISP, tales como incompatibilidades de tecnología, deficiencias en el sistema eléctrico comercial, averías (físicas / lógicas), falta de soporte técnico, errores o factores humanos, etc. El plan deberá incluir la participación y

responsabilidades de cada una de las áreas involucradas así como el debido procedimiento de prueba (simulacro).

- Desarrollar manuales de procedimiento de configuración (administradores) y uso (usuarios) de servicios, equipos y sistemas del ISP; mismos que deberán ser socializados, comunicados y aplicados por el personal respectivo.

- Desarrollar manuales de procedimiento de almacenamiento de información, que consideren el esquema de clasificación de datos, extracción de respaldos, mantenimiento de dispositivos, etc.

- Disponer de un sitio alterno para el almacenamiento de información de respaldo; con la infraestructura adecuada para evitar la degradación de los soportes de almacenamiento; y las seguridades física y lógica necesarias.

- Desarrollar un manual de procedimiento de contrataciones y adquisiciones con los lineamientos necesarios para el establecimiento de bases y especificaciones técnicas (de ser el caso), garantías, soporte, etc.

- Suscribir contratos o convenios de soporte técnico (24/7) y mantenimiento con los respectivos proveedores y/o con empresas especializadas; debiendo establecerse todas las formalidades del caso como son, suscripción de actas entrega – recepción, niveles de servicio, ejecución de protocolos de prueba para la recepción de servicios, sistemas y/o equipos, etc.

- Diseñar e implementar un sistema de seguridad industrial acorde a la realidad y requerimientos de la empresa.

- Ejecutar, en ambientes de prueba controlados, estudios y/o investigaciones formales relacionadas con las capacidades de los recursos de la empresa: equipos y servicios de comunicaciones y de información; con el fin minimizar el riesgo a degradaciones o interrupciones en el servicio.

- Establecer un sistema que permita efectuar un seguimiento y reporte de cambios de configuraciones en servicios y sistemas, en el cual cada usuario y su actividad pueda ser identificada de manera única y ser almacenada en un repositorio central para la obtención de información procesada para la toma de decisiones.

- Suscribir contratos de aseguramiento patrimonial que cubran a los equipos críticos del ISP.

- **TAREA TR 1.2. Preparar e implementar planes de tratamiento**

La implementación de las recomendaciones planteadas por el equipo evaluador es responsabilidad de la Gerencia de la empresa tomada como caso de estudio. La implementación de planes de tratamiento no se encuentra dentro del alcance del presente estudio.

5.3. Evaluación de hipótesis

Tal como se explicó en el Capítulo IV, numeral 4.5, la aplicación de la presente propuesta metodológica para la gestión de riesgos tecnológicos permite a las empresas proveedoras de Internet (ISP) contar con indicadores sobre los cuales tomar decisiones de control y por consiguiente minimizar dichos riesgos.

Esta situación es evidente en el presente capítulo, en el cual para la empresa del caso de estudio se ha obtenido la LISTA DE RIESGOS PRIORIZADOS (Anexo 10), misma que se constituye y contiene los indicadores a partir de los cuales se generaron opciones de control destinadas a la minimización de riesgos (Fases No. 3 y 4 de la propuesta metodológica).

Por su parte, la minimización de riesgos tecnológicos se evidencia en la estimación del Nivel de Riesgo Residual Neto que resulta inferior a los Niveles de Riesgo Residual Actual; tal como se presenta en el Anexo 11.

CAPITULO VI

6.1. Conclusiones.

En la investigación realizada a la muestra de los ISP de la ciudad de Quito se determinó el grado de madurez con el cual dichas empresas administran sus riesgos tecnológicos; obteniéndose que éste se encuentra por debajo de un valor que pueda considerarse “Administrable”.

La propuesta metodológica para la gestión de riesgos tecnológicos planteada genera indicadores para la toma de decisiones de control por parte de las Gerencias de las empresas a las cuales está orientada. Dichos indicadores se reflejan en la LISTA DE RIESGOS PRIORIZADOS, la misma que se obtiene durante el proceso de aplicación de esta metodología.

La propuesta metodológica para la gestión de riesgos tecnológicos desarrollada se ajusta al escenario local sobre la cual fue planteada, por cuanto emplea procedimientos de estimación de riesgos que resultan adecuados ante el deficiente nivel de madurez y la falta de datos históricos con que los ISP de la ciudad de Quito gestionan sus riesgos.

La propuesta metodológica para la gestión de riesgos tecnológicos planteada se aplicó en una empresa ISP representativa de la ciudad de Quito. Esto permitió la demostración de la hipótesis trazada, usando para ese cometido, datos e información real obtenida de la situación actual de dicha empresa.

Sobre la base de la LISTA DE RIESGOS PRIORIZADOS obtenida para la empresa del caso de estudio se derivaron controles recomendados que contribuyen a la gestión de los riesgos tecnológicos en dicha empresa. Sin embargo, como se explicó antes, la implementación de esos controles escapa del alcance de este estudio.

6.2. Recomendaciones.

Se recomienda a las empresas proveedoras de servicio de Internet de la ciudad de Quito acoger la propuesta metodológica para la gestión de riesgos tecnológicos que se presenta en este trabajo; con el objetivo de alcanzar mejores niveles de madurez en su gestión y consecuentemente potencializar su competitividad; factores que se reflejarán en una adecuada calidad de servicio para el cliente/abonado – usuario final.

Es recomendable se implementen los controles que deriven de la aplicación de la metodología de gestión de riesgos a fin de evitar pérdidas directas dentro de la organización así como la afectación a los servicios utilizados por terceros e incluso sanciones por parte de los entes regulatorios y de control. Para tal efecto, es imprescindible el apoyo de la Gerencia General como base para los programas de educación, entrenamiento e implementación de los procesos de gestión de riesgos.

Se recomienda a las entidades de regulación y de control del sector de las telecomunicaciones en el Ecuador, incentiven en las empresas proveedoras de servicios la implementación de programas, acciones y/o políticas de gestión de riesgos tecnológicos toda vez que el nivel de dependencia a la tecnología de dichas empresas las obligaría a mantener controles efectivos que salvaguarden sus inversiones y consiguientemente garanticen la calidad del servicio final.

Se recomienda a las empresas ISP investigar y conocer las diferentes metodologías que permiten administrar los riesgos tecnológicos e involucrar y capacitar en ello al personal necesario con el propósito de que dichos procesos empiecen a tratarse dentro de la organización y se tome conciencia de su importancia.

Se recomienda que, en la medida de lo posible, dentro de las empresas proveedoras de servicios de telecomunicaciones se conforme un Comité de Seguridad de la Información encargado de documentar y monitorear cada fase de la implementación, con la capacidad de considerar cambios, actualizaciones y ajustes a un entorno propio de cada empresa y de supervisar los procesos relacionados.

CITAS

(Castro, 2012)

(Valenciana, 2012)

(Díaz, 2009)

(Isaca, 2009)

(The Institute, 2008)

(ISO/IEC27005, 2008)

(ISO/IEC27000, 2009)

(INEN-ISO/IEC27005, 2012)

(The Institute, GTAG 6, 2008)

(The Institute, GTAG 11, 2008)

(Castro, TI, 2012)

(Enisa, 2006)

(ISO31000, 2009)

(Pallas, 2009)

(SIGWEB, 2001)

REFERENCIAS BIBLIOGRÁFICAS

Castro, A. (2012). *Riesgo tecnológico y su impacto para las organizaciones parte I.* Obtenido de http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i.

Castro, A. (2012). *TI.* Obtenido de Riesgo tecnológico y su impacto para las organizaciones parte II Gobierno de TI y riesgos: http://revista.seguridad.unam.mx/numero-15/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-ii-gobierno-de-ti-y-riesgos

Díaz, M. (2009). *Análisis de Riesgos: ISO 27005 vs Magerit y otras metodologías.* Obtenido de http://www.delitosinformaticos.com/10/2009/proteccion-de-datos/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias#.USTb02clZvk

Enisa. (2006). *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools.* Obtenido de http://www.enisa.europa.eu/rmra/rm_home.html.

INEN-ISO/IEC27005. (2012). NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27005. *Técnicas de seguridad – Gestión del riesgo en la seguridad de la Información* .

Isaca. (2009). COBIT® 4.1. *Modelos de Madurez* .

ISO/IEC27000. (2009). Information Technology. *Security Techniques - Information security management systems* .

ISO/IEC27005. (2008). Information Technology. *Security Techniques - Information Security Risk Management Standard* .

ISO31000. (2009). *Gestión de Riesgos – Principios y Guías.* Obtenido de http://www.fecoopse.com/files/iso_31000_-_gestion_de_riesgos_-_espaol.pdf

Pallas, M. G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Obtenido de http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

SIGWEB. (2001). *Matriz de Riesgo, Evaluación y Gestión de Riesgos*. Obtenido de http://www.sigweb.cl

The Institute, I. A. (2008). GTAG 11. *Developing the IT Audit Plan* .

The Institute, I. A. (2008). GTAG 4. *Gestión de la auditoría de tecnología de la información* .

The Institute, I. A. (2008). GTAG 6. *Gestión y auditoría de puntos vulnerables de tecnología de la información* .

Valenciana, S. d. (2012). *Manual de Fiscalización Sección 315.3: Guía de aplicación: El conocimiento requerido del control interno de la entidad.* Obtenido de http://www.sindicom.gva.es/