UNIDAD DE GESTIÓN DE POSTGRADOS

MAESTRÍA DE EVALUACIÓN Y AUDITORIA DE SISTEMAS DE LA II y III PROMOCIÓN

TESIS DE GRADO MAESTRÍA DE EVALUACIÓN Y AUDITORÍA DE SISTEMAS

TEMA: "*MODELO DE EVALUACIÓN Y MONITOREO DEL CUMPLIMIENTO DE CONTROLES DE GESTIÓN TECNOLÓGICO PARA EL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO*"

Autores:

Ing. Jacqueline Genoveva Lala Guevara

Ing. Luis Daniel López Guilcapi

Director:

Ing. Jaime Meza

SANGOLQUÍ, junio de 2014

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

ING. JAIME MEZA
DIRECTOR

ING. ESTEVAN GÓMEZ
OPONENTE

CERTIFICAN

Que el trabajo titulado "MODELO DE EVALUACIÓN Y MONITOREO DEL CUMPLIMIENTO DE CONTROLES DE GESTIÓN TECNOLÓGICO PARA EL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO" realizado por: Lala Guevara Jacqueline Genoveva y López Guilcapi Luis Daniel, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidos por la ESPE, en el Reglamento Estudiantes de las Universidades de las Fuerzas Armadas ESPE.

Debido a que el presente trabajo es el Diseño del modelo de Evaluación y Monitoreo, que permitirá al Municipio del Distrito Metropolitano de Quito identificar los controles, procesos que mantiene la institución y los que requieren mayor atención para mejorar la eficacia y disminuir el riesgo, acompañado con jornadas de monitoreo en el cumplimiento de las políticas y a una toma de decisiones de la Institución.

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

Autorizan a Lala Guevara Jacqueline Genoveva y López Guilcapi Luis Daniel, a entregar el mismo a la Unidad de Gestión de Postgrados.

Sangolquí, 20 junio del 2014

ING. JAIME MEZA
DIRECTOR

ING. ESTEVAN GOMEZ
OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACION Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA DE EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

PROMOCIÓN III – IV

DECLARACIÓN DE RESPONSABILIDAD

Lala Guevara Jacqueline Genoveva

López G. Luis Daniel

DECLARAMOS QUE:

El proyecto de grado denominado "MODELO DE EVALUACIÓN Y MONITOREO DEL CUMPLIMIENTO DE CONTROLES DE GESTIÓN TECNOLÓGICO PARA EL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO", ha sido desarrollado en base a una investigación, respetando derechos intelectuales de terceros, conforme a las citas que constan el pie de las páginas 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 grado en mención.

Sangolquí, 20 junio del 2014

Lala Guevara Jacqueline Genoveva López Guilcapi Luis Daniel

DEDICATORIA

Jacqueline lala:

A Dios todo poderoso

A mis padres, mis hermana(o)s

A mi familia (Micaela(hija), Milton)

Luis López:

A Dios y a mí familia en especial a mi madre Rocío, quien siempre me ha apoyado para alcanzar mis metas propuestas.

AGRADECIMIENTO

El desarrollo de este proyecto se hizo posible con la colaboración y aportes de algunas personas que invirtieron tiempo, esfuerzo y dedicación.

Al Ing. Jaime Meza, MAE Tutor Académico, Ing. Estevan Gómez MBA Oponente designado por habernos orientado y apoyado en la aplicación de la metodología necesaria y requerida para el desarrollo de este estudio.

A mi compañera /(o) de tesis con quien se compartió ideas, inquietudes y soluciones para el desarrollo del proyecto enfocados a alimentarnos de información y a titularnos como maestrantes.

A mis compañeros de clases, por colaborar suministrándonos sugerencias para la realización de la estructura del presente trabajo; y por todos los buenos momentos compartidos, en especial a mi compañero (a) de tesis.

A mis profesores de la maestría, por impartirnos los conocimientos tan valiosos e importantes para poder aportar lo aprendido en el estudio de este proyecto, en especial: Mario Ron.

Al personal del Municipio del Distrito Metropolitano de Quito- Dirección Metropolitana de Informática, compañeros de trabajo y excelentes profesionales con cuales se comparte día a día, nuevas experiencias y conocimientos y por la colaboración prestada en todo momento, para el desarrollo de este trabajo.

INDICE

INDICE DE TABLAS

INDICE DE ECUACIONES

RESUMEN

Las tecnologías de la información y las comunicaciones (TICs) implementadas en las instituciones han hecho necesario crear políticas de gestión de tecnología para el uso del mismo, pero éstas en su mayoría no son implementadas completamente ni correctamente; para lo cual se plantea un Modelo de Evaluación y Monitoreo de las **Políticas de Gestión Tecnológica** del MDMQ – DMI; este trabajo presenta un estudio que tuvo como propósito el Diseño de un Modelo de Evaluación de las políticas de la DMI, enfocado en los controles de la Norma ISO 27000; el primer capítulo presenta la identificación del problema; el segundo presenta el estudio y análisis de las normas, técnicas, y estándares que rigen los temas de seguridad; el tercer capítulo se presenta la **investigación de campo** para realizar el levantamiento de información a través de encuestas, revisiones en campo para determinar las vulnerabilidades, amenazas que tiene el área de tecnología, de ésta manera se determina la situación actual del cumplimiento de políticas en el MDMQ y DMI; el cuarto capítulo presenta el resultado de la situación actual que tiene el área de Tecnología, la cual se utilizó para realizar experimentaciones y determinar en cuál de los once dominios de la **ISO27002** se puede disminuir el riesgo, utilizando valores de exposición que permitieron identificar el riesgo por dominio y finalmente obtener el mejor nivel de exposición que determina el **modelo de evaluación y monitoreo del cumplimiento de controles de gestión tecnológico** apoyado en la metodología de uso que permitirá evaluar el riesgo en el área de tecnología (DMI).

Palabras clave:

- Políticas de Gestión Tecnológica del MDMQ
- Modelo de evaluación y monitoreo.
- Cumplimiento de controles de gestión tecnológico.

ABSTRACT

The information technology and communication (ICT) implemented in the institutions have made it necessary to create policies to manage technology for the use of it, but mostly they are not fully or properly implemented; for which a Monitoring and Evaluation Model of Technological Management Policy MDMQ arises - DMI; This paper presents a study that aimed at the design of an Evaluation Model DMI policies, controls focused on the ISO 27000 standard; The first chapter presents the identification of the problem; the second presents the study and analysis of the rules, techniques, and standards governing safety issues; The third chapter presents field research for gathering information through surveys, field reviews to determine vulnerabilities, threats to the area of technology, in this way the current state of policy compliance is determined at the MDMQ and DMI; The fourth chapter presents the results of the current situation that has the technology area, which was used to conduct experiments to determine which of the eleven domains of ISO27002 can reduce risk, using exposure values which identified risk by domain and finally get the best level of exposure that determines the model evaluation and monitoring of compliance with management controls technology supported methodology that will allow use risk assessment in the area of technology (DMI).

Keywords:

-
  - Policy Management Technology MDMQ
  - Model evaluation and monitoring.
  - Compliance with management controls technology.

CAPITULO I

1. Introducción

La Dirección Metropolitana de Informática en el 2011, genera políticas de gestión tecnológica para estandarizar los procedimientos implementando controles, la política fue difundida en las dependencias afines, administraciones zonales, pero de acuerdo a la documentación evidenciada en el proceso de relevamiento de información no existe control continuo que verifique el cumplimiento de las políticas, por lo tanto, luego de haber realizado el análisis de los resultados obtenidos de las encuestas se constató que la institución no dispone de un modelo guía que apoye a gestionar el control y una mejora continua en las actividades de control y evaluación tecnológica de las dependencias desconcentradas de la Dirección Metropolitana de informática.

En base a ésta premisa, la investigación tiene como propósito diseñar un modelo de monitoreo y control basado en estándares internacionales y que cumpla con las directrices establecidas por los entes rectores de control interno, puesto que de acuerdo a la Resolución A 10 la Dirección Metropolitano de Informática se encuentra bajo el nivel de gestión sectorial representada por la Administración Generala del Municipio de Quito

En el presente desarrollo de tesis se analizó la normativa vigente evaluando la eficacia de los controles de gestión tecnológica, luego se realizó el diagnóstico de la situación actual de la DMI referente al cumplimiento de las políticas establecidas, de ésta manera se analiza los riesgos al incumplimiento de las políticas existentes con lo cual se definió un modelo de gestión tecnológico que permita estandarizar los controles proactivos en las dependencias que conforman el Municipio de Distrito Metropolitano de Quito utilizando normativas vigentes y estándares internaciones; seguidamente se realizó experimentos para validar el modelo disminuyendo los niveles de riesgos en la mayoría de los casos tecnológicos.

1.1 Planteamiento del problema

El Municipio del Distrito Metropolitano de Quito, dentro del su plan Metropolitano de Desarrollo establece ejes estratégicos que permitan estructurar de manera integral, articulada, sistemática con proyección hacia el 2022; el plan cuenta con objetivos, políticas, metas y programas, dentro de los cuales establece a la tecnología como un eje trasversal para la consecución de sus objetivos, es así que mediante instrumentos administrativos (resolución aA0010) se establece a la Dirección Metropolitana de Informática como el ente rector para emitir políticas que apoyen a la Gestión Tecnológica en respuesta a brindar información oportuna, utilizable, confiable con prácticas efectivas y productivas.

Si bien es cierto la Dirección Metropolitana de Informática cuenta dentro de su plan estratégico proyectos que persiguen asegurar los activos de información los mismos que se encuentran bajo la guía estándar de PMBOK 4, pero no existe un modelo estándar que permita su aplicación y monitoreo continuo, de tal forma que minimice los riesgos de explotación de vulnerabilidades por amenazas latentes en el medio de forma proactiva y que este alineado con el plan de ***riesgos aprobado***, esta situación genera un conjunto de problemas tales como:

- Emisión de informes con salvedades por parte de los órganos de control (Auditoría Interna/Contraloría) que determinan inobservancia en la aplicación de controles en uso de la tecnología municipal.
- Los funcionarios técnicos de la municipalidad tanto a nivel de la dirección como de las dependencias desconcentradas y, los usuarios de los sistemas de información, por desconocimiento o por dar solución inmediata a requerimientos, alteran datos y hacen que la información no sea confiable incumpliendo uno de los principios promulgados en la ISO 27000 que es la integridad, esta situación genera que los usuarios realicen actividades fuera de sus competencias.
- La asignación y control de acceso a Soluciones TIC, y servicios tecnológicos a usuarios sin autorización previa de los Directores respectivos pone en riesgo que la información confidencial o sensitiva quede a disposición de personas que

brinden mal uso a la información lo que puede llevar a que los órganos de control generen recomendaciones de incumplimiento.

- Falta de indicadores de monitoreo y control de servicios no permitan mantener un control continuo de la disponibilidad de la plataforma.

De continuarse observando este tipo de comportamientos, el MDMQ, en particular las áreas de gestión y administración de Recursos de TI estaría incumpliendo funciones, deberes y obligaciones que le competen, aumentando el riesgo a las vulnerabilidades en la parte tecnológica e incurriendo en faltas administrativas y disminuyendo el nivel de confianza al área de TI convirtiéndose en una área netamente operativa y de alto riesgo en la gestión de tecnologías.

Con la creación y correcta aplicación de un modelo de evaluación y monitoreo para el cumplimiento de controles de gestión Tecnológica se va a apoyar a mantener Seguridad física y lógica, continuidad del negocio, correcta administración de cambios, pruebas específicas de control interno permitiendo tener una correcta gestión y administración de TI en las dependencias del MDMQ.

1.2 Justificación e Importancia

El Municipio del Distrito Metropolitano de Quito dentro de su plan de gobierno Ordenanza N° 0170, establece a la tecnología de la información como un elemento de apoyo transversal de la gestión de gobierno local, dentro de la cual la seguridad de información y los controles en el uso de las TIC´s, hacen imprescindible la necesidad de contar con un modelo de Evaluación y monitoreo de su cumplimiento de forma continua, el mismo que será una herramienta apegada a la realidad municipal, que permita estar acorde a los estándares y la normativa vigente para la mejora continua en las actividades de control y evaluación de las dependencias del Municipio de Distrito Metropolitano de Quito.

El objetivo del presente proyecto es la creación de un modelo de control que se ajuste a los estándares internacionales y que cumpla con las directrices establecidas por los entes rectores de control tecnológico como lo es la Contraloría General del Estado a través de acuerdo N° 039, con el propósito que cubra los objetivos de control sobre la efectividad, eficiencia de las operaciones, confiabilidad de la

información y cumplimiento con las leyes y regulaciones aplicables a la Dirección Metropolitana de Informática y por ende a las áreas tecnológicas que se encuentran sectorizados que son parte del Municipio de Quito.

Además el desarrollo del presente modelo de control contribuirá a la mejora en la Seguridad de la Información y efectividad de los controles en el uso de las TIC´s a nivel municipal, estableciendo un referente metodológico y teórico a seguir por los municipios del país coadyuvando al cumplimiento de los objetivos planteados en el Plan Nacional del Buen Vivir.

1.3 Formulación del problema a resolver.

- ¿Cuáles son los modelos teóricos y o empíricos que permiten establecer modelos y estándares de control y seguimiento de gestión de TI?
- ¿Cuál es el estado actual del Municipio del Distrito Metropolitano de Quito, a nivel de madurez de aplicación de las mejores prácticas de aseguramiento y monitoreo?
- ¿Cuál es la mejor solución que va a permitir a la Dirección Metropolitana de Informática, la implementación de controles proactivos en relación con las mejores prácticas de control interno basados en la normativa vigente?

1.4 Hipótesis

Disminuir los niveles de riesgo de los controles en la mayoría de los casos tecnológicos establecidos por la DMI en el MDMQ, a través de un modelo de Evaluación y monitoreo del cumplimiento de controles de gestión Tecnológica adaptado a la realidad municipal.

1.4.1 Determinación De Variables

- Variable Independiente

La **causa** es identificar si los controles actualmente implementados son eficaces y eficientes, acorde a la normativa vigente que mantiene la institución.

- Variable Dependiente

El efecto que se quiere alcanzar en la introducción de la variable dependiente, es el diseño de un modelo de control que permita identificar los niveles de riesgo en la

aplicación de controles tecnológica (a mayor control menor riesgo), mejorando y promoviendo la visión de la DMI.

1.5 Metodología

La presente tesis utiliza la metodología documental, de campo y experimental.

- Documental ya que el análisis de la información que se obtiene se basa en diversas fuentes de información, (Bejarano Ramos, Galarza Chiriboga, Rivera Moncayo , Ceballos , & Moncayo), ya que se utiliza las políticas de Gestión Tecnológicas de la Dirección Metropolitana de Informática del Distrito Metropolitano de Quito y normas internacionales.
- De campo ya que el tema de estudio sirve como fuente de información al investigador, (Bejarano Ramos, Galarza Chiriboga, Rivera Moncayo, Ceballos , & Moncayo), para lo cual se utilizó las encuestas.
- Experimental ya que se realizan una serie de pruebas para observar su comportamiento, (Bejarano Ramos , Galarza Chiriboga , Rivera Moncayo , Ceballos , & Moncayo), en el presente trabajo re realizo cambios experimentales a la variable independiente para asi ver el comportamiento del riesgo total.

1.6 Objetivo General

Crear un modelo de Evaluación y monitoreo del cumplimiento de los controles de gestión Tecnológica en el Municipio del Distrito Metropolitano de Quito MDMQ, a fin de establecer un marco de referencias estándar para la aplicación de controles de gestión tecnológica en sus dependencias.

1.6.1 Objetivos Específicos

- Analizar la normativa vigente, referencias bibliográficas, teóricas y prácticas donde se establecen los estándares de control interno y seguimiento de Gestión de TI, para evaluar la eficacia de los controles aplicados en la gestión e tecnología, a través de aplicación de métodos de investigación.
- Realizar el diagnóstico de la situación actual de la Dirección Metropolitana de Informática y de los ejes estratégicos institucionales, referente al cumplimiento de las políticas establecidas. para determinar el nivel de madurez de riesgos en la

aplicación de controles de IT; utilizando la normativa vigente mediante el análisis documental de información histórica de control y de aplicación de métodos de investigación en campo.

- Definir un modelo de control tecnológico que permita estandarizar los controles proactivos en las dependencias que conforman el Municipio del Distrito Metropolitano de Quito.
- Establecer los experimentos y métodos que permitan validar el modelo sobre una muestra aplicable, a fin de poder demostrar la validez de la hipótesis planteada, mediante la utilización de modelos matemáticos y estadísticos formalmente aceptados.

1.7 Alcance

El ámbito de estudio del presente trabajo, es amplio en el sentido de identificar el estado actual del riesgo que presenta la institución en los diferentes ámbitos que tiene la tecnología, por lo tanto se presenta a la Dirección Metropolitana de Informática un modelo de control y evaluación basada en la norma de Seguridad de la Información (ISO 27002), la misma que va a determinar los controles de alto riesgo de criticidad, para luego ser tratados con mayor atención, identificando los controles que se apeguen a las necesidades del negocio.

CAPITULO II

2. Marco Teórico

2.1 Control en las Organizaciones

Un control interno es un proceso mediante el cual los directivos proporcionan a las actividades de un grado razonable de confianza (COSO, COMMITTEE OF SPONSORING ORGANIZATIONS, 2004), de tal forma que garantice la consecución de sus objetivos estratégicos, tomando en cuenta: la eficacia y eficiencia de las operaciones, fiabilidad de la información, cumplimiento de leyes y normas aplicables, con la finalidad de dotar a la institución medidas preventivas, detección y corrección de errores, fallos y fraudes.

Hoy en día, la tecnología de la información está presente en las áreas de la organización (DeLaFuente, 2000), puesto que la implantación de controles sin planificación resulta bastante costoso (Carolina Benavides, 2011). Sin embargo la creciente dependencia del uso de las Tics y la complejidad de las medidas para el aseguramiento de sistemas de información en la institución se ha visto necesaria generar normas, políticas y por ende a controles con un fin, mantener un control tecnológico en la organización de ésta manera minimizar las brechas de riesgos, por lo tanto, en base a la problemática existente el aplicar controles en las áreas de tecnológica es una necesidad fundamental debido a que un incidente generado puede tener un impacto directo en el cumplimiento de sus objetivos.

Es así que en apoyo a las políticas tecnológicas existen marcos de referencia de Control que se encargan del control y administración de las tecnologías de información apoyando a realizar el control interno en medianas y pequeñas instituciones proporcionando bases claras para toma de decisiones, realizando periódicamente una evaluación del funcionamiento de las tecnologías de la información al interior de la institución.

2.2 Estándares y normas del Cumplimiento de políticas

El Ecuador presenta marco regulatorio pero cuenta con normativa reducida en el campo tecnológico, y como ente mandatorio sobre las instituciones gubernamentales se encuentra la Contraloría General del Estado la cual se ve apoyada en el campo tecnológico es por ello que se toma coma base las normas y estándares internacionales a fin de establecer lineamientos que garanticen el cumplimiento de los objetivos institucionales.

El Control en la tecnología de información es el inicio en el proceso de implementación de un marco de referencia estándar que apoye al control manteniendo el objetivo de la institución; razón por la cual los marcos de referencia se han convertido en el insumo de decisiones para la directiva los mismos que apoyan a reducir los riesgos que amenazan a la información.

Entre los estándares más conocidos en temas de tecnología son los siguientes:

- **COBIT**.- Conjunto de Mejores Prácticas para el manejo de información, creado por Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI) en 1992 (ISACA, 2011); se enfoca en el alineamiento de los objetivos de negocio, control y auditoría para Tecnología de Información y Comunicación.
- **ITIL** (Information Technology Infrastructure Library). Conjunto de conceptos y prácticas para la gestión de servicios, el desarrollo y/o las operaciones relacionadas con las tecnologías de la información (APM_Group, 2007) selecciona las mejores prácticas en administración de servicios de Tecnología de Información.
- **COSO**.- La norma acrónimo de The Committee of Sponsoring Organizations Of the Treadway Commission (Estructura conceptual integrada, 2000), presenta recomendaciones a los responsables de Tecnología de Infomación para evaluar e implementar sistemas de control, centrando el objetivo en la efectividad y la eficiencia de las actividades, cumplimiento de regulaciones, valoración de riesgos y actividades de control.

- **Magerit** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas). Metodología de carácter público del Ministerio de Administraciones Públicas de España. Fue elaborado por el Consejo superior de administración pública (Dirección General para el Impulso de Electrónica, 2011)(Dirección General para el Impulso de la Administración Electrónica, 2011); presenta indicadores de control que permite identificar posibles riesgos que existan en el área de TI.
- **ISO SERIE 27000**.- Es el estándar publicado por la Internacional Organization for Standardization (ISO); la norma define requerimientos y proporciona directrices que orientan a mantener la gestión de seguridad de información; el cual tiene como objetivo identificar zonas críticas de TI para iniciar, mantener e implementar la seguridad de la información en una organización.

2.2.1 COBIT, Control Objectives for Information and Related Technology

COBIT es un marco de referencia fundamentada en los objetivos de control y se encuentra alineado con otros estándares de control como COSO.

COBIT es un marco de referencia y tiene como objetivo los requerimientos de negocio en cuando a la eficiencia, efectividad, integridad, disponibilidad, confidencialidad y cumplimiento (COBIT, CRITERIOS DE INFORMACIÒN DE COBIT, 2007); limita a objetos de control de alto nivel de acuerdo a las necesidades de negocio, por lo tanto, el logro es posible a través de definición de controles.

Misión de COBIT.- "Investigar, desarrollar, hacer público y pro- mover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento", (COBIT, 2007)

Objetivos De Control. Es el resultado que se quiere alcanzar implementando procedimientos de control tecnológicos. COBIT presenta 34 objetivos de control para los procesos de tecnología agrupados en cuatro dominios: Planeación y organización, adquisición e implementación, entrega y monitoreo.

Usuarios de COBIT.- COBIT apoya con soluciones a Administradores, usuarios y auditores (COBIT, 2007). A los administradores les provee de una base teórica para su toma de decisiones, apoya en la definición de un PETI (Plan estratégico de tecnología de información) del cual se desglosa una definición de arquitectura, adquisición de software, aseguramiento de servicio, supervisión del funcionamiento.

Los usuarios les proveen el tratamiento de la información. A los auditores les permite identificar temas de control dentro de la infraestructura de la empresa, ver Figura 1.

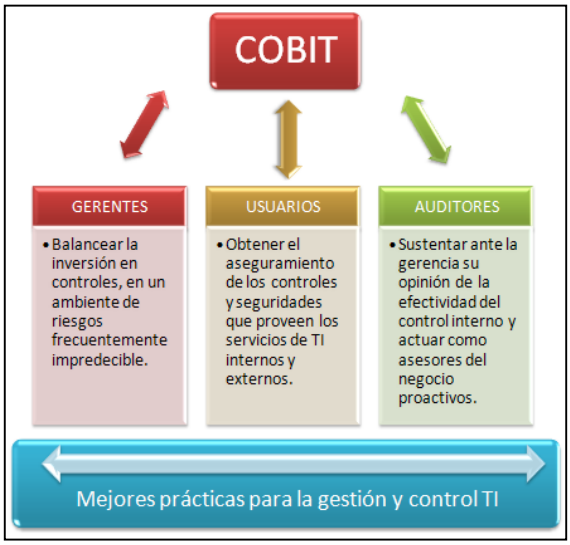

Figura 1. Usuarios COBIT, (Rodríguez, 2010)

2.2.1.1 Modelo de trabajo de COBIT.

El modelo de COBIT relaciona a los objetivos de función de servicio con los requerimientos de información. Los procesos de COBIT permite a las actividades de

TI ser administradas y controladas por los objetivos de control de COBIT, Ver Figura 2.

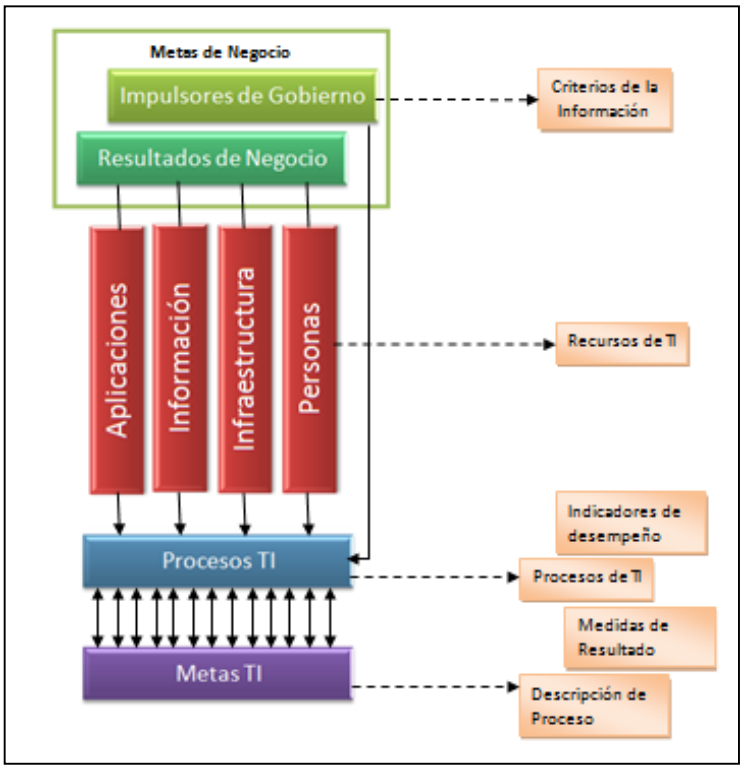

Figura 2. Modelo De Trabajo Cobit (Cobit, Criterios De Informaciòn De Cobit, 2007)

Los recursos de TI son manipulados por procesos de TI para cumplir con las metas de TI que responden a requerimientos de la empresa. De acuerdo a COBIT este es el principio básico de trabajo, como se ilustra en el cubo de COBIT, Ver Figura 3.

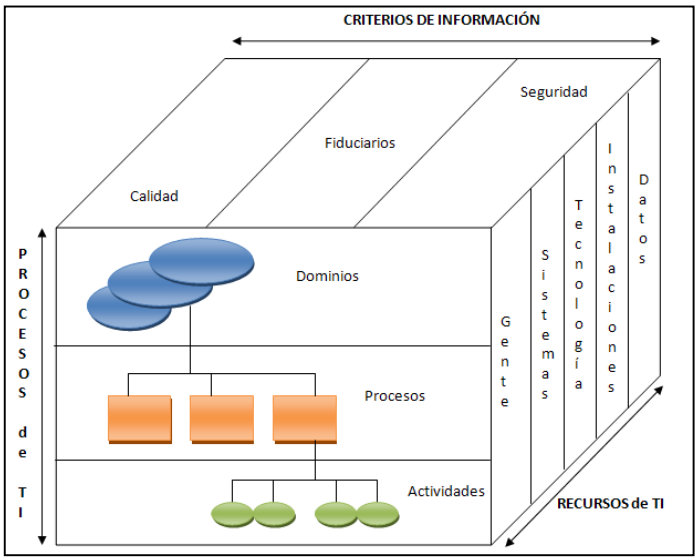

Figura 3. Cubo de COBIT (COBIT, 2007, pág. 47)

Criterios de Información.- Para tener información que satisfaga los requerimientos de negocio, utiliza ciertos criterios:

Requerimientos de Calidad.- Costo, entrega, efectividad, eficiencia, cumplimiento de leyes y regulaciones.

Requerimientos de Seguridad.- Confidencialidad, integridad y disponibilidad.

Recursos de TI

COBIT establece los recursos en TI para alcanzar los objetivos de negocio: tecnología, sistemas, datos, recurso humano.

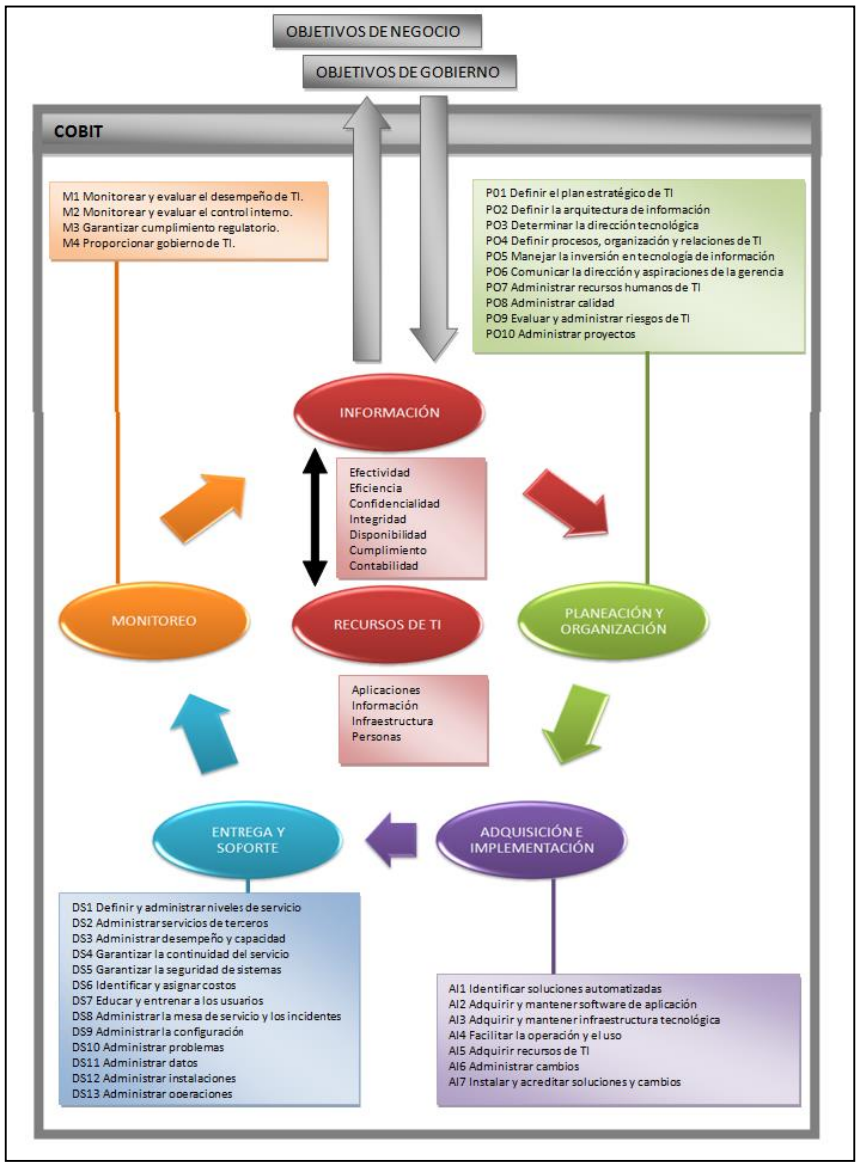

Figura 4, Marco de Trabajo Completo de COBIT (COBIT, 2007)

2.2.1.2 Procesos de TI.

COBIT se divide en tres niveles:

- **Dominios**.- Agrupación de procesos, corresponde a una organización organizacional.
- **Procesos**.- Conjunto de actividades unidas por controles.
- **Actividades**.- Acciones utilizadas para obtener un resultado medible.

2.2.2Information Technology Infraestructure Library, ITIL

ITIL es un conjunto de mejores prácticas para la gestión de servicios de TI (ITIL V3); la versión de ITIL mostrada en la Figura 5, tiene como objetivo desarrollar procedimientos efectivos y económicos, uno de sus objetivos es alinear los objetivos de servicio a los objetivos de negocio.

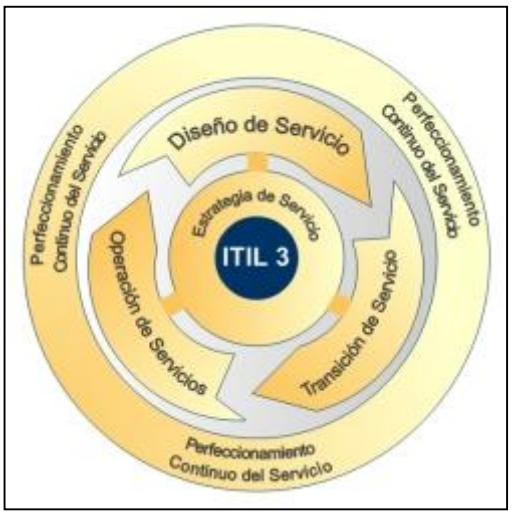

Figura 5, ITIL versión 3 (APM_Group, 2007)

2.2.2.1 Ciclo de Vida de los Servicios de TI

La versión ITIL 3 en su estructura de gestión de servicios tiene como objetivo ofrecer una visión global de la vida de un servicio desde el diseño del servicio. El ciclo de vida del Servicio, ver Figura 6, contiene cinco fases correspondientes a los nuevos libros de ITIL:

- **Estrategia del Servicio**: Trata a la gestión de servicio como un activo estratégico, permite desarrollar una estrategia en la Organización respecto a Tecnología de Información.
- **Diseño del Servicio**: Abarca los principios y métodos requeridos para transformar los objetivos estratégicos en portafolios de servicios y activos.
- **Operación del Servicio**: cubre las mejores prácticas para la gestión del día a día en la operación del servicio de la Organización acorde a las necesidades de los clientes.

- **Mejora Continua del Servicio**: Proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a través de un diseño, transición y operación del servicio optimizado.
- **Transición del Servicio**: Abarca el proceso de transición para la implementación de nuevos servicios o su mejora.

Figura 6, Ciclo de Vida de ITIL (APM_Group, 2007)

ITIL crea una integración de procesos de TI, personas y herramientas dentro de la estrategia de negocios a través de los servicios de TI. La estructura que mantiene describe como los procesos están conectados, determina el comportamiento permitiendo organizar la infraestructura diseñada para un rendimiento sustentable.

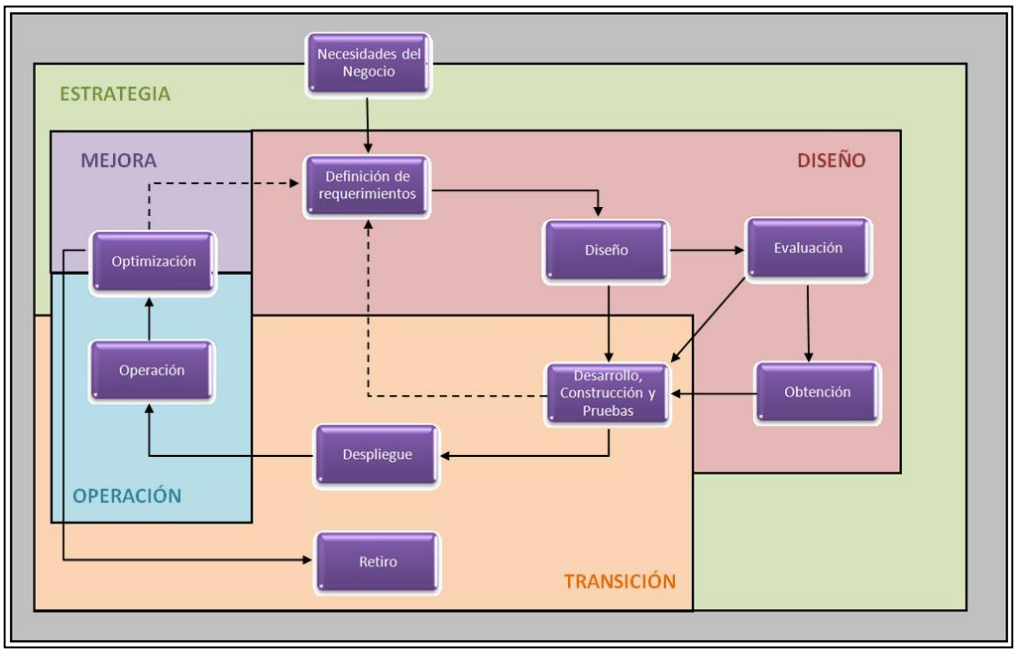

Figura 7, Procesos de ITIL (APM_Group, 2007)

2.2.3 COSO

COSO I fue un informe sobre control interno elaborado en 1992, con el objetivo fundamental de especificar un marco conceptual de control interno de las organizaciones, capaz de integrar las políticas con los lineamientos que permita a la alta dirección mejorar el control interno. COSO I se basa en los siguientes componentes: ambiente de control, evaluación de riesgos, actividad de control, información y comunicación y supervisión.

COSO II tiene como enfoque el mismo que el COSO Report pero basado en el riesgo; éste enfoque permite a las organizaciones mejorar las prácticas de control interno.

Marco del Control Interno (COSO-ERM) se define como el *proceso que ejecuta la administración con el fin de evaluar operaciones específicas con seguridad razonable en tres principales categorías: Efectividad y eficiencia operacional, confiabilidad de la información financiera y cumplimiento de políticas, leyes y normas.* (COSO, COMMITTEE OF SPONSORING ORGANIZATIONS, 2004).

El marco integrado de control que presenta COSO-ERM consta de ocho componentes relacionados e integrados al proceso de gestión, siendo estos componentes los siguientes: ambiente interno, establecimiento de objetivos, identificación de eventos, evaluación de riesgos, respuesta al riesgo, actividades de control, información y comunicación, y supervisión.

En COSO existe una relación directa entre los objetivos y los ocho componentes referenciados que se manifiestan permanentemente en el campo de la gestión: las unidades operativas y cada agente de la organización conforman secuencialmente un esquema orientado a los resultados. Los componentes de COSO se muestran en la Figura 8.

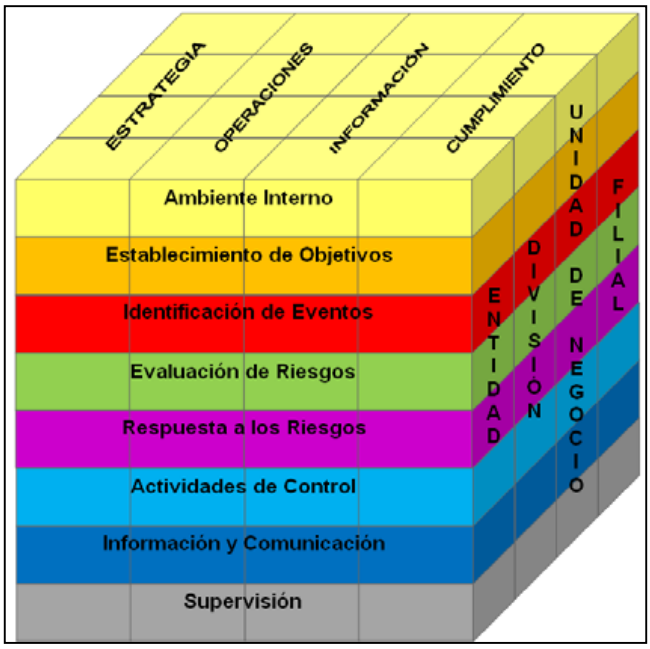

Figura 8. Componentes de COSO (COSO, 2009)

Entre cada componente existe una relación entre la información de forma ascendente, descendente con el objetivo de que los directivos mantengan la

comunicación con las áreas de control. La Figura 9 muestra los flujos de información entre las actividades inherentes.

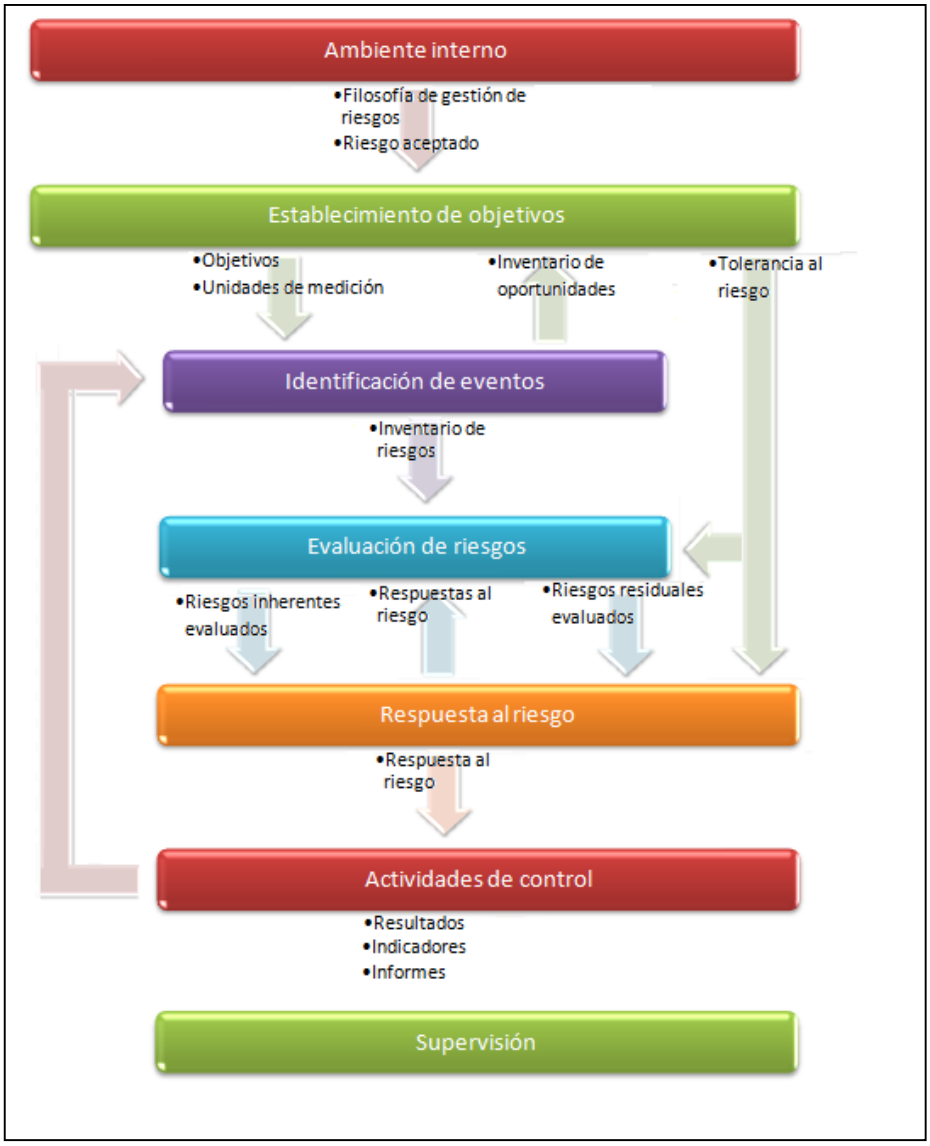

Figura 9, Flujo de Información ERM. (COSO, 2009)

2.2.4 MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) estudia los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que exista un daño o perjuicio; y segundo recomienda las medidas apropiadas que deben adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

MAGERIT, como método de análisis y gestión de riesgos, cubre la fase de la gestión global de la seguridad de un sistema de información.

La gestión global de seguridad, representada en la Figura 10.

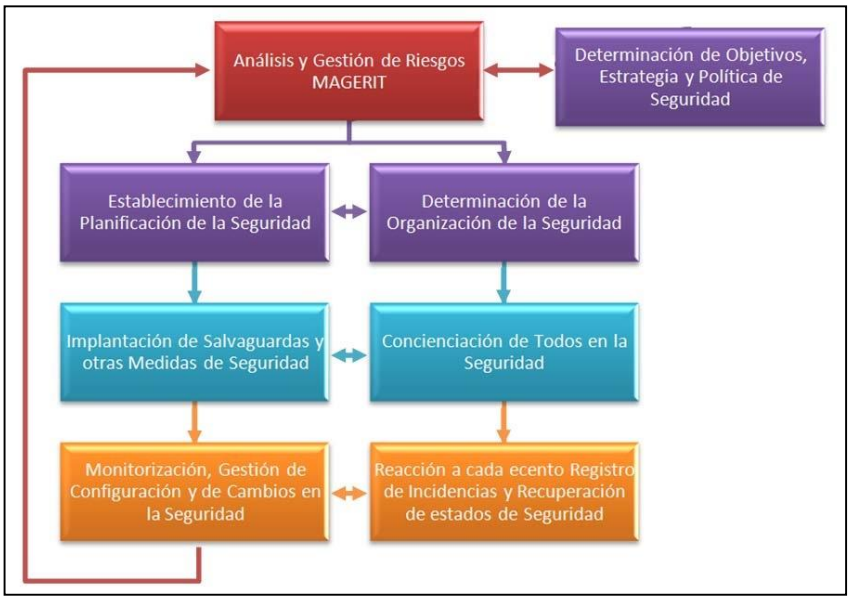

Figura 10, Análisis y Gestión de Riesgos MAGERIT, (MAGERIT 1, 2012)

MAGERIT maneja una visión global sobre la seguridad de los Sistemas de Información de las Administraciones Públicas, el modelo presenta tres submodelos correspondiente a elementos, eventos y procesos, Ver Figura 11.

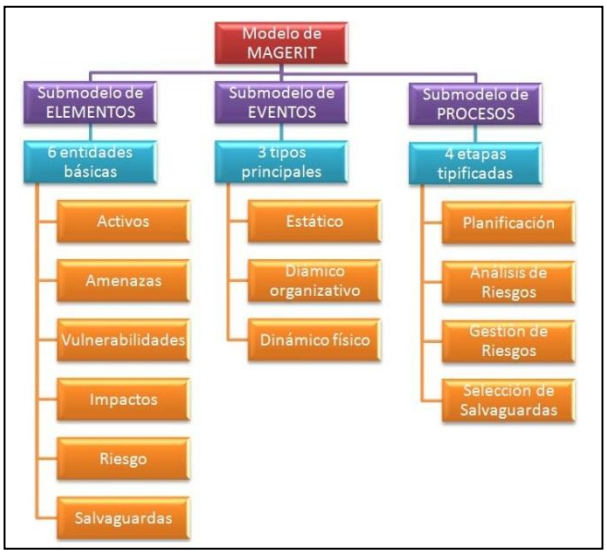

Figura 11, Modelo de Magerit. (MAGERIT 1, 2012)

2.2.5 NORMAS ISO 27000

Las normas ISO/27000 constituyen una serie de estándares desarrollados por la International Organization Standarization (ISO), también conocida como "la familia de estándares de gestión de seguridad de la información", proporciona una serie de recomendaciones y mejores prácticas sobre gestión de la seguridad de la información, gestión de riesgos y controles, en el contexto de un Sistema de Gestión de Seguridad de la Información (SGSI).

La serie ISO/IEC 27000 consta de un gran número de partes publicadas que se consideran básicas y que son las que se muestran en la Tabla 1.

Tabla 1,

Normas básicas de la serie ISO/IEC 27000.

Norma	Título
ISO/IEC 27000:2009	Information security management systems - Overview and vocabulary
ISO/IEC 27001:2005	Information security management systems - Requirements
ISO/IEC 27002:2005	Code of practice for information security management
ISO/IEC 27003:2010	Information security management system implementation guidance
ISO/IEC 27004:2009	Information security management - Measurement
ISO/IEC 27005:2011	Information security risk management
ISO/IEC 27006:2011	Requirements for bodies providing audit and certification of information security management systems

Fuente: Normas básicas de la serie ISO/IEC 27000, (Calafat)

La ISO 27000 está formado por varias series, entre ellas se menciona las siguientes:

ISO 27001.- Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

La norma ISO/IEC 27001:2005 Information security management systems – Requirements (ISO27000 2005a).- Mantiene un enfoque basado en procesos y especifica los requisitos para la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI), dentro del contexto los requisitos establecidos en esta norma son aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza.

Esta norma internacional sigue el ciclo PDCA, que se aplica para estructurar todos los procesos del sistema de gestión de seguridad de la información. La Figura 12 muestra el SGSI propuesto por la norma ISO/IEC 27001.

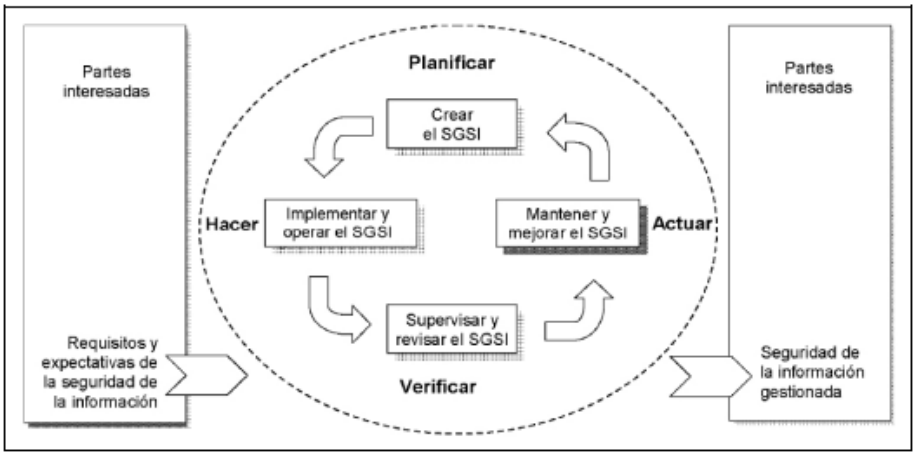

Figura 12. SGSI de la norma ISO/IEC 27001 (ISO 27001, 2005)

27002:2005 Code of practice for information security management. - Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. La norma establece las directrices y los principios generales para iniciar, implantar y mantener la gestión de la seguridad de la información en una organización así como para fortalecer la confianza a la hora de llevar a cabo actividades inter organizacionales.

Los objetivos y controles de la norma proporcionan una guía general sobre las metas de gestión de la seguridad de la información, contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Ver Tabla 2

Tabla 2, Estructura de la norma ISO/IEC 27002

Estructura de la norma ISO/IEC 27002

Dominios	Objetivo de Control	Controles
Política de seguridad	1	2
Aspectos organizativos de la Seguridad de Información	2	11
Gestión de activos	3	5
Seguridad ligada a los recursos humanos	2	5
Gestión de comunicaciones y operaciones	10	32
Control de acceso	7	25

Continúa →

Adquisición, desarrollo y mantenimiento de los sistemas de Información	6	16
Gestión de Incidentes de seguridad de Información	2	5
Gestión de la continuidad del negocio	1	5
Cumplimiento	3	10
Total	**39**	**133**

Fuente: Normas de la ISO/IEC 27002

Cada categoría contiene un objetivo, que expone aquello que se pretende conseguir, la descripción de cada control se estructura en tres campos diferentes: descripción del control, directrices para su implantación y otra información adicional.

ISO 27003.- Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO 27004.- La norma actúa como una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables que determina la eficacia de un SGSI.

ISO 27005.- La norma proporciona directrices para la gestión del riesgo en la Seguridad de la Información, apoya a los conceptos específicos de la norma ISO/IEC 27001.

2.3 Riesgo

Al riesgo se le define estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización (MAGERIT V3,2012), es la manera de cuantificar el incumplimiento del objetivo planteado lo que representa ganancias o pérdidas para la institución y según la Organización Internacional por la Normalización (ISO) define riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando

vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños".

En base a esta definición el riesgo tecnológico se plantea como amenaza que podría afectar al core de negocio tal sería el caso de pérdida de información.

En la definición realizada al riesgo existen varios componentes que son parte del riesgo, los mismos que se detallan a continuación:

- **Probabilidad**.- Establece la probabilidad de que pueda ocurrir el evento, el cual puede ser cuantitativo o cualitativo.
- **Amenazas**.- Las amenazas son existentes en nuestro entorno y por lo general son aquellas que pueden causar consecuencias; en el ámbito tecnológico son eventos que pueden producir daños dando como resultado pérdidas materiales (equipos) o pérdida de información.
- **Vulnerabilidades**.- Son debilidades existentes en los sistemas de Información que pueden potenciar a la amenaza para causar daños y producir pérdidas en la institución.
- **Activos**.- Representado por aquellos que se relacionan con los sistemas de información tales como equipos, infraestructura, software y el más importante los datos.
- **Impacto**.- Se enfoca a la magnitud del daño que podría ser causado si las amenazas explotan a la vulnerabilidad.
- **Nivel de Impacto**.- Se determina por el impacto causado en el logro de la misión. Eje.: Sensibilidad de los datos.

2.3.1 Riesgos de Tecnología de Información

El riesgo de Tecnología de Información se lo podría definir como el efecto de una causa que se incrementa por la frecuencia de ocurrencia dentro del entorno de Tecnología. En así que surge la necesidad de tener controles que actúen sobre el riesgo minimizando los efectos.

2.3.2 Gestión del Riesgo

Desde el inicio de los sistemas informáticos han existido riesgos y no se ha tomado en cuentas a las seguridades ya sea en recurso humano, organizacional, infraestructura; en el transcurso del tiempo las instituciones han visto la necesidad de implementar métodos, políticas y herramientas que apoyen a implementar la Seguridad informática en los procesos operativos de ésta manera se alinea a las estrategias que tiene la institución, para proteger y garantizar el cumplimiento de los objetivos institucionales.

Las instituciones constantemente sufren ataques de virus, y de los propios funcionarios quienes acceden a la información con facilidad y utilizan los datos obtenidos para beneficio propio.

2.3.2.1 Gestión del Riesgo en la Seguridad Informática

La gestión de riesgo se presenta como la forma de determinar, analizar, valorar y clasificar los riesgos.

Los riesgos provienen de una amplia variedad de fuentes pero las normas de gestión del riesgo han sido desarrolladas por varias organizaciones, entre ellas COBIT, ISO, MAGERIT. Estos estándares están diseñados para apoyar a la organización a identificar formas de reducir los riesgos.

2.3.3 Valoración del Riesgo

La valoración de riesgo se basa en los criterios básicos, el alcance y límites de la Organización, de acuerdo a la ISO-IEC-27005 los riesgos deben ser identificados de forma cualitativa o cuantitativa priorizando los criterios de evaluación del riesgo y los objetivos estratégicos de la Organización. La valoración tiene como principio determinar el valor de los activos de la información de ésta manera permite identificar las vulnerabilidades y amenazas existentes o que podrían existir, de la misma manera identifica controles existentes y los efectos del riesgo, de acuerdo a la ISO 27005, con la información generada permite determinar consecuencias potenciales priorizando los riesgos, clasificando los riesgos de evaluación del riesgo.

De acuerdo al Anexo E de la ISO 27005, presenta el enfoque para la valoración del riego definiendo la prioridad y la cronología de las acciones como la valoración a alto nivel a través del cual y de acuerdo al presupuesto podrá o no ser implementado los controles respectivos. La probabilidad de ocurrencia de una amenaza es que la susceptibilidad de la vulnerabilidad explote; de acuerdo a la ISO 27005, Anexo E.2.1 los métodos de valoración de riesgo de éste tipo, los activos físicos o de software se evalúan en términos de costos de compra, cambio o reconstrucción y luego se convierte en escala cualitativa.

La valoración de la información se obtiene a través de entrevistas a personas seleccionadas de la gerencia quien es la autoridad para definir el valor y la sensibilidad de los datos y el acceso a darse.

La valoración se logra utilizando lineamientos de valoración de información y los temas relacionada según ISO 27005 son los siguientes:

- Seguridad personal
- Información personal
- Obligaciones legales
- Cumplimiento de la Ley
- Intereses comercial
- Pérdida financiera/alteración de actividades
- Orden Público
- Políticas y operación de negocio
- Etc.

Los lineamientos para valorar un activo se realizar en escala numérica y puede ser tomada entre 0 a 4, lo que permite reconocer un valor cualitativo o cuantitativo, de la misma manera los valores de las amenazas y vulnerabilidades se toma en cuenta para la valoración del activo por lo tanto la probabilidad de la amenaza puede ser **alta, media o alta.** Ver Figura13

	Probabilidad de ocurrencia - Amenaza	Baja			Media			Alta		
	Facilidad de explotación	B	M	A	B	M	A	B	M	A
Valor del activo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Figura 13, Valoración de un activo (ISO 27005, Tabla E.1 a)

La probabilidad de un incidente frente al impacto en el negocio se presenta porque la amenaza explota la vulnerabilidad, de tal forma que el riesgo es medido en escala de 0 a 8 que se evalúa frente a los criterios de aceptación del riesgo, por lo tanto, de acuerdo a Figura 14, presenta la escala riesgo de la siguiente forma:

- Riesgo bajo: 0-2
- Riesgo medio: 3-5
- Riesgo alto: 6-8

	Probabilidad del escenario de incidente	Muy baja (muy improbable)	Baja (Improbable)	Media (Posible)	Alta (Probables)	Muy alta (Frecuente)
Impacto en el negocio	Muy baja	0	1	2	3	4
	Baja	1	2	3	4	5
	Media	2	3	4	5	6
	Alta	3	4	5	6	7
	Muy alta	4	5	6	7	8

Figura 14, Tabla E.1 b (27005:2012, 2012)

La valoración del riesgo según la ISO 27005, presenta el análisis de riesgo quien presenta las siguientes actividades:

- Identificación del riesgo
- Estimación del riesgo
- Evaluación del riego

2.3.3.1 Identificación del riesgo

De acuerdo a la ISO/ IEC 27001, numeral 4.2.1 d, permite identificar los activos, identificando el propietario, responsable de su producción, mantenimiento, uso y

seguridad; el resultado es un listado de activos que van a ser parte de la gestión del riesgo.

Los activos de información se pueden representar a ficheros, base de datos, contratos, manuales, equipos informáticos, servicios informáticos, personas, como se muestra en la Figura 15.

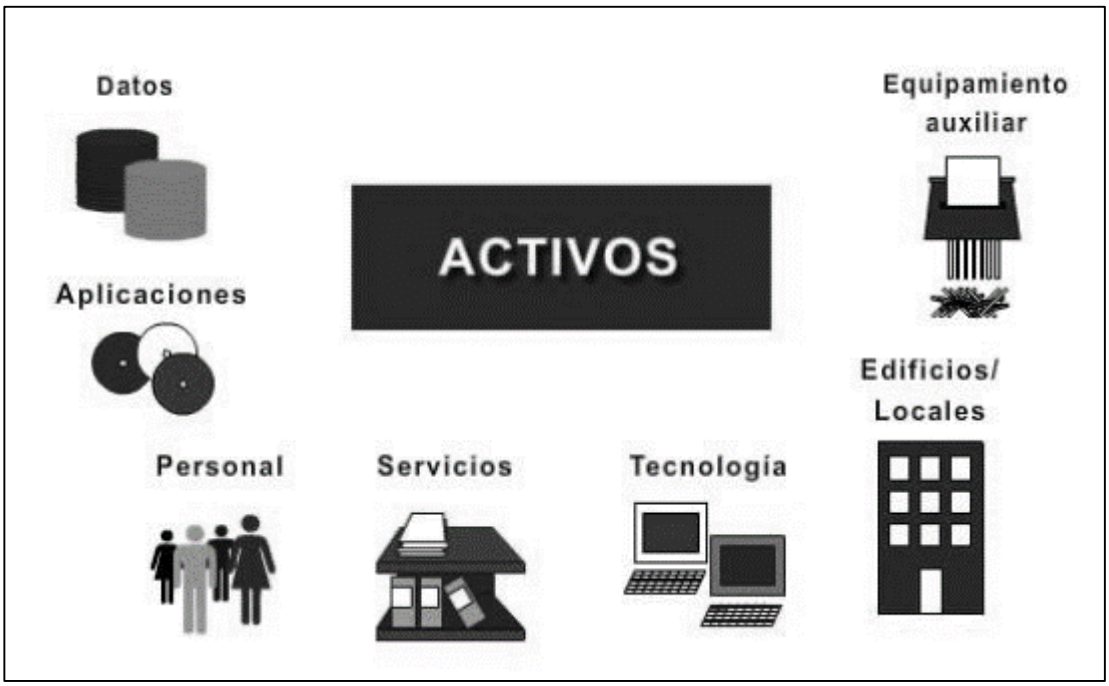

Figura 15, Activos de Información, (27005:2012, 2012)

De acuerdo a la ISO 27005, Anexo B se identifican a los activos de la siguiente forma:

Activos Primarios:

- Información.
- Procesos del negocio

Activos de soporte:

- Hardware
- Software
- Redes
- Estructura de la Organización

2.3.3.2 Estimación del riesgo

El análisis de riesgo puede presentarse en varios grados de criticidad del activo, de acuerdo a la (ISO 27005, Metodología para la estimación del riesgo), puede ser cualitativa o cuantitativa.

- **Estimación cualitativa**.- presenta la escala de atributos que describen las consecuencias potenciales de un riesgo (alta, media, baja).
- **Estimación cuantitativa**.- presenta una escala con valores números, tomando como base, información de fuentes existentes.

2.3.3.3 Evaluación del riesgo

La evaluación presenta el listado de riesgos con niveles de valor asignado los cuales son determinados al establecer el contexto, la ISO 27005(Anexo E) determina que para evaluar los riesgos las organizaciones deben comparar los riesgos estimados con el criterio de evaluación del riesgo.

2.3.4 Identificación de amenazas

La información de amenazas se obtiene de los propietarios de los activos, incidentes u otras fuentes, puede causar daños a activos (información, procesos y sistemas), las amenazas pueden ser causales o accidentales y definidos por el tipo de amenaza (acceso no autorizado, daño físico, etc) de acuerdo a la ISO 27005, Anexo C; el resultado es un listado de amenazas con la identificación del tipo de amenaza.

2.3.5 Identificación de los controles

La información de los controles se identifican verificando los existentes evitando costos innecesarios, para lo cual las revisiones por parte de reportes de auditoría entrega información respecto a la eficacia del control, el resultado es el listado de controles existentes y planificados.

2.3.6 Identificación de vulnerabilidades

La información se obtiene de las amenazas, activos y los controles existentes los cuales se obtiene en las áreas de Organización, Procesos y procedimientos, rutinas de

gestión, personal, Ambiente físico, Hardware, software, Configuración del Sistema de Información. Las vulnerabilidades y métodos de valoración se encuentran en el Anexo D de la ISO 27005.

2.4 Estadística

La Estadística es la parte de las Matemáticas que se encarga del estudio de un conjunto de muestras de en una población, recogiendo los datos, organizándolos en tablas, representándolos gráficamente y analizándolos para sacar conclusiones de dicha población, (Calmaestra, 2005). Permite realizar el análisis de las características de un conjunto de muestras para poder determinar las características comunes entre ellas.

2.4.1 Muestra

La muestra es una parte representativa de una determinada población, (Calmaestra, 2005). Para el análisis estadístico existen se pueden utilizar:

- Medidas de Centralización.
- Medidas de dispersión.

2.4.1.1 Medidas de centralización

Las medidas de centralización son aquellas que nos permiten representar por medio de un solo número el conjunto de datos, es decir, dar valor representativo, (Triola, 2009)

Entre las medidas de centralización tenemos:

- Media
- Media ponderada

2.4.1.2 Media

"La media de un conjunto de observaciones muéstrales se representa con el símbolo $\overline{x}$. Intuitivamente, la media simboliza el "centro de masas" o "punto de equilibrio central" del conjunto de datos considerado", (Juan, Fuente, & Vila, 2011, pág. 18). El valor representa el valor más representativo de un conjunto de muestras.

El cálculo de la media de un conjunto de datos se usa la siguiente fórmula:

$$\bar{x} = \frac{x_1 + x_2 + \ldots + x_n}{n} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

Ecuación 1 formula de la media, (Juan, Fuente, & Vila, 2011, pág. 3)

2.4.1.3 Media Ponderada

"La media ponderada es una medida de tendencia central, se construye asignándole a cada clase un peso, y obteniendo un promedio para los pesos", (Estevez & Estevez, 2003). La media ponderada es el valor medio de la muestra, en la que cada una de las muestras posee su propio peso.

La fórmula para el cálculo de la media ponderada es la siguiente:

$$\bar{x}_w = \frac{\sum_{i=1}^{n} (w_i x_i)}{\sum_{i=1}^{n} w_i}$$

Ecuación 2 Formula de la media ponderada, (Estevez & Estevez, 2003)

Donde

- *wi* = valor de peso para *xi* o ponderación
- *xi* = dato i

2.4.2 Medidas de dispersión

Las medidas de dispersión son aquellas que nos ayudan a observar el comportamiento de una serie estadística, (Gorgas, Cardiel, & Zamorano, 2009), para así poder conocer el grado de desviación con respecto a la serie, para lo cual se tiene la varianza, la desviación típica o estándar.

2.4.2.1 Desviación estándar

La desviación estándar es un índice numérico de la dispersión de un conjunto de datos o población, (Tecnológico de Monterrey, s.f.). La desviación estándar permite identificar que tan separados se encuentran los datos de la media.

La fórmula para el cálculo de la desviación estándar es la siguiente:

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_n - \bar{x})^2}{N}}$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{N}}$$

Ecuación 3 Desviación estándar, (Vitutor, 2012)

2.4.2.2 Coeficiente de Variación

El coeficiente de variación es la relación entre la desviación típica de una muestra y su media, (Vitutor, 2012). El coeficiente de variación permite comparar que dispersos se encuentran dos distribuciones distintas, cuando los valores siempre sean positivos.

Para el cálculo del coeficiente de variación se utiliza la siguiente fórmula:

$$C.V = \frac{\sigma}{\bar{x}}$$

Ecuación 4 Coeficiente de variación, (Vitutor, 2012)

CAPITULO III

3 Metodología de análisis y valoración

Luego del análisis inicial de la presente investigación se acordó con la Dependencia DMI realizar una reunión de inicio en la cual con el apoyo del Director, se conocieran detalles de las áreas involucrados que aplica las políticas de Gestión Tecnológica de la DMI en el que se determinó las áreas, perfiles, los productos o servicios que tiene cada unidad.

Una vez finalizada la reunión, se acuerda la directriz de análisis de riesgo a ser empleada (ISO 27000) y los criterios de evaluación a utilizarse, además de definir las dependencias idóneas en la que se va a analizar los riesgos contemplando el tiempo a realizarse en cada entrevista bajo un cronograma de las fechas de las visitas técnicas.

3.1 Metodología

La valoración de riesgo en la presente investigación permitió determinar las amenazas potenciales y riesgos asociados con los activos de información; permitió identificar los controles que van a permitir mitigar o eliminar el riesgo.

El riesgo presentado en la investigación es el resultado del impacto por el valor del resultado de la encuesta al cual determinamos como Indicador, el cual representa al control que mantiene tecnología en uno de sus componentes.

La probabilidad en la investigación representa al indicador como un valor cualitativo obtenido de las encuestas; se determina como un evento favorable o desfavorable dependiendo de la pregunta tecnológica; en cada ítem de la encuesta se determina la amenaza, la vulnerabilidad potencial y el control que se aplica actualmente, de ésta forma se determina si está acorde a las políticas de gestión tecnológica de la DMI.

El impacto en la investigación se determina como los activos tecnológicos más relevantes que mantiene la institución tales como servicios, datos/ información, aplicaciones, equipos informáticos, redes de comunicaciones, instalaciones; la información referencial es obtenida de fuentes primarias que tiene como custodio el

Municipio de Quito quienes son los custodios de la información; el impacto se determina por el valor potencial cuantitativo que tiene la misión de la institución.

La metodología de valoración de riesgos aplicada a la investigación se detalla en la Figura 16, que fue determinada por (Bautista, Plan de Seguridad de la Información Compañia XYZ Soluciones, 2013), la misma que se compone de las siguientes actividades:

- Caracterización del contexto
- Identificación del activo y sus amenazas
- Identificación de vulnerabilidades
- Análisis de controles
- Determinación de probabilidades
- Análisis de impacto
- Determinación de riesgos

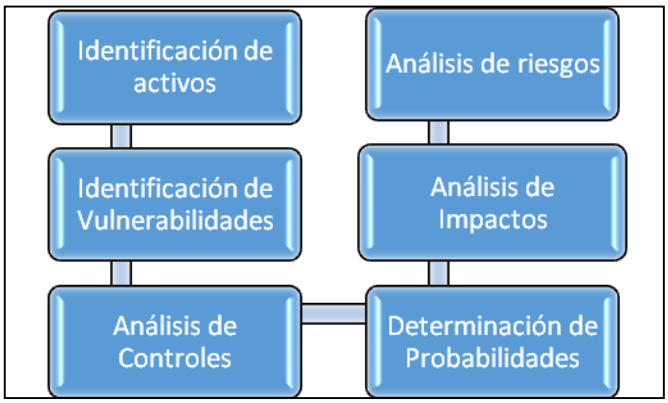

Figura 16, Valoración del riesgo, (Bautista, Alcance del proyecto, 2013)

3.2 Caracterización del contexto evaluado

En ésta actividad definir el alcance del esfuerzo y el límite del ejercicio para ejecutarlo, se requiere de la identificación de elementos tales como hardware, software, datos de información para conocer el contexto a ser evaluado.

3.3 Identificación de Activos y Amenazas

La fuente de amenaza se define como una circunstancia o evento potencial que va a causar daños a la información. Las fuentes comunes de amenazas son las

personas, la naturaleza; según la norma ISO/IEC 27005, Anexo C determina una lista de ejemplos de amenazas comunes que están agrupados en varios tipos, tales como:

- Daño físico.
- Eventos naturales.
- Pérdida de servicios.
- Perturbación debido a la radiación
- Fallas técnicas, entre otras.

Los activos de información del proceso se los identifica y clasifica de acuerdo a la criticidad (Disponibilidad, Confidencialidad y Disponibilidad), los recursos se agrupan de acuerdo las funciones, para luego ser revisados dentro de un ciclo continúo de valoración de riesgos y poder determinar las amenazas relevantes. Ver Figura 17, Ciclo de Valoración y Estimación del riesgo.

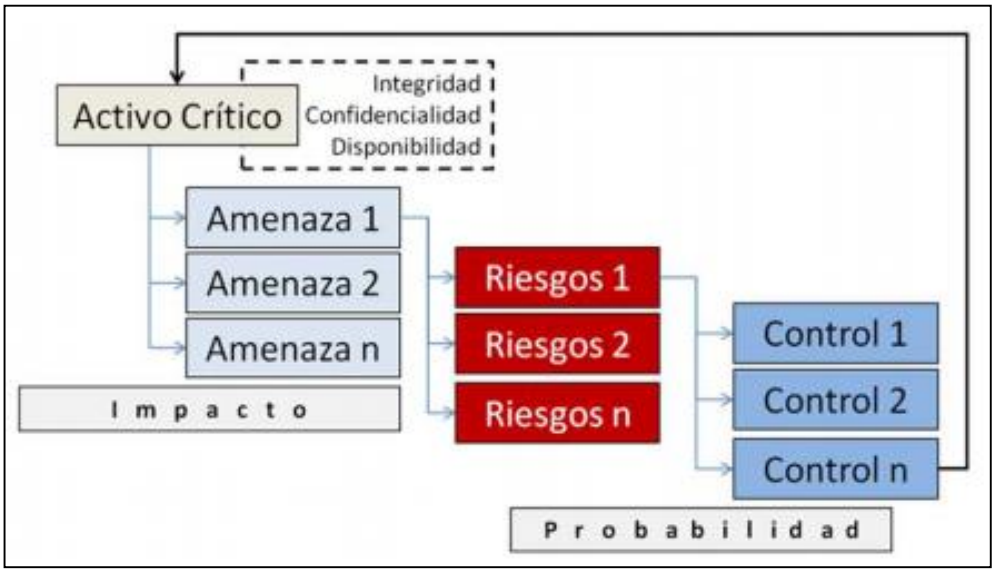

Figura 17, Ciclo de valoración y estimación del riesgo, (Bautista, Alcance del proyecto, 2013)

De acuerdo al apoyo del Director en el que sugirió que se use como norma de apoyo la ISO 27000, se determinó algunas de las amenazas aplicables al contexto que se encuentran en la ISO/IEC 2005, de ésta manera se facilita el proceso de levantamiento de información durante las entrevistas, las mismas que se detallan a continuación:

- Fuego

- Acciones laborales
- Fallas de hardware
- Acceso físico no autorizado
- Causas naturales (terremoto, inundación, etc)
- Fallas de suministro
- Causas ambientales
- Señales de interferencia
- Espionaje
- Intrusión
- Hurto de información
- Hurto de equipos
- Recuperación de medios reciclados.
- Divulgación
- Manipulación de Hardware
- Manipulación de Software
- Deterioro de equipos
- Fallas de software
- Incumplimiento en el mantenimiento del SI
- Uso no automatizado del equipo
- Uso de software no licenciado
- Errores humanos
- Abuso de derechos
- Negación de acciones.

3.4 Identificación de Vulnerabilidades

Las vulnerabilidades actúan por una debilidad en los procedimientos de seguridad, diseño, implementación generando una brecha de seguridad.

Análisis de Controles.- Los controles pueden o no ser técnicos. El control técnico es la protección implementada al hardware, software o firmware; en cambio

controles no técnicos pueden ser controles administrativos, operacionales tales como políticas de seguridad, procedimientos operacionales.

Determinar probabilidades.- Para determinar las vulnerabilidades se deben tener en cuenta los siguientes factores:

- Naturaleza de la vulnerabilidad.
- Existencia y eficacia de los controles existentes.
- Motivos de la fuente de amenaza.

La escala de medición establecido en la probabilidad de una vulnerabilidad puede ser explotada por una fuente de amenaza, y de acuerdo a la (ISO/IEC27001, numeral4.1), determina el porcentaje de riesgos identificados evaluados como de su importancia alta, media, o baja. Ver Tabla 3

Tabla 3.

Valoración de Probabilidad

PROBABILIDAD		
Descripción	**Calificación**	**Explicación**
Alto	5	100% Alta, certeza, siempre ocurre.
Medio Alto	4	75% Mayor, probable, se espera que ocurra
Medio	3	50% Se espera que no ocurra regularmente
Medio Bajo	2	25% No esperado, pero podría ocurrir algunas veces
Bajo	1	10% Remoto, puede ocurrir en circunstancias excepcionales.

Fuente: ISO/IEC27001, numeral 4.1

3.5Análisis de Impacto

Al impacto se describe como la degradación de una o varias metas de seguridad que afecten a la (Integridad, Disponibilidad y Confidencialidad). Ver Tabla 4.

- **Pérdida de Integridad**.- La integridad se pierde cuando se presenta modificaciones no autorizadas en los datos o sistemas.
- **Pérdida de Disponibilidad**.- La falta de disponibilidad en un sistema afecta a los usuarios finales, incumpliendo el objetivo de institución.
- **Perdida de Confidencialidad**.- La confidencialidad de la información se refiere a divulgación no autorizada.

Tabla 4, Valoración del Impacto

Valoración del Impacto

IMPACTO	
Escala	**Definición**
Alto	Muy alto, la explotación de la vulnerabilidad puede resultar pérdidas financieras.
Medio Alto	Alto, pérdida financiera significativa disminuyendo la imagen de la institución.
Medio	Medio, Pérdida financiera moderada, afectando en bajo nivel la imagen de la institución.
Medio Bajo	Bajo, pérdida financiera
Bajo	Menor, costos asociados bajos

Fuente: ISO/IEC27001

En base al levantamiento de información para determinar el inventario de activos que tiene el área de tecnología del MDMQ, como parte del inventario es la información que se encuentra custodiada en los servidores de la DMI(catastral, financiera, nómina, Gestión catastral, etc), la valoración cuantitativa determinada por el personal entrevistado del área de Tecnología se presenta en el ANEXO2, en la que se presenta la siguiente información:

- **Servicios**
  - Servicio de pago en línea de los impuestos por medio de instituciones financieras (Teller, SAO, PATENTES).
- **Datos / Información**
  - Información (Catastral, Financiera, Nómina, Ordenamiento Territorial, etc) almacenada en las bases de datos en oracle spacial, oracle, sql server,
  - El código fuente de los sistemas se encuentra versionado en los servidores de la DMI.
- **Aplicaciones**
  - Aplicativos de recaudación municipal, catastral, seguridad(SIREC-Q, SGCT,SLUM, TRANSFERENCIA DE DOMINIO, IRM, etc.)
- **Equipos informáticos**

- Servidor físicos, virtuales, switch, router , firewall, IPS, IDS, etc.

- **Redes de comunicaciones**
  - Dispositivos de comunicación de red local, telefónica, inalámbrica.
- **Soporte de Información**
  - Storage, discos duros.
- **Instalaciones**
  - Data center de la DMI y dependencias desconcentradas.
- **Equipamiento auxiliar**
  - Cintas de almacenamiento, etc.

La escala cuantitativa de los activos de información del MDMQ, se detalla en la Tabla N° 5.

Tabla 5

Impacto Cuantitativo de los activos de información de la DMI,

Escala Cualitativa	Descripción
Alto	Más de $32.000.001 mensuales
Medio Alto	de $ 24.000.001 - $32.000.000
Medio	de $16.000.0001 - $24.000.000
Medio Bajo	Hasta $16.000.001
Bajo	Hasta $800.000

Fuente: López & Lala, 2013

3.6Determinación de Riesgos

Para determinar el nivel de riesgo que presentan los activos de información de la Institución referente a tecnología se representa en función de:

- La probabilidad de que una fuente de amenaza intente explotar una vulnerabilidad.
- La efectividad de controles existentes para reducir o mitigar los riesgos.

Para determinar el nivel de riesgo inherente se multiplica los valores de la probabilidad de una amenaza por los valores de impacto, como se muestra en la Figura 18.

Mapa del Riesgo del Proyecto							
IMPACTO	ALTA	5	5 Zona tolerable, Reducir el riesgo, Compartir o transferir	10 Zona riesgo moderado, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	15 Zona de riesgo inaceptable, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	20 Zona de riesgo inaceptable, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	25 Zona de riesgo inaceptable, Reducir el riesgo, Evitar el riesgo, Compartir o transferir
	MEDIA ALTA	4	4 Zona aceptable, Reduce el riesgo, Compartir o transferir	8 Zona tolerable, Reducir el riesgo, Compartir o transferir	12 Zona riesgo moderado, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	16 Zona de riesgo inaceptable, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	20 Zona de riesgo inaceptable, Reducir el riesgo, Evitar el riesgo, Compartir o transferir
	MEDIA	3	3 Zona aceptable, Reduce el riesgo, Compartir o transferir	6 Zona tolerable, Reducir el riesgo, Compartir o transferir	9 Zona riesgo moderado, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	12 Zona riesgo moderado, Reducir el riesgo, Evitar el riesgo, Compartir o transferir	15 Zona de riesgo inaceptable, Reducir el riesgo, Evitar el riesgo, Compartir o transferir
	MEDIA BAJA	2	2 Zona aceptable, Reduce el riesgo, Compartir o transferir	4 Zona aceptable, Reduce el riesgo, Compartir o transferir	6 Zona tolerable, Reducir el riesgo, Compartir o transferir	8 Zona tolerable, Reducir el riesgo, Compartir o transferir	10 Zona riesgo moderado, Reducir el riesgo, Evitar el riesgo, Compartir o transferir
	BAJA	1	1 Zona aceptable, Reduce el riesgo, Compartir o transferir	2 Zona aceptable, Reduce el riesgo, Compartir o transferir	3 Zona aceptable, Reduce el riesgo, Compartir o transferir	4 Zona aceptable, Reduce el riesgo, Compartir o transferir	5 Zona tolerable, Reducir el riesgo, Compartir o transferir
			BAJA	**MEDIA BAJA**	**MEDIA**	**MEDIA ALTA**	**ALTA**
			1	**2**	**3**	**4**	**5**
			0 - 20%	**21 - 40%**	**41 - 60%**	**61 - 80%**	**81 - 100%**
			PROBABILIDAD				

Figura 18. Mapa del Riesgo para el desarrollo del Proyecto, (27005:2012, 2012)

La escala del riesgo se define por los niveles: Alto, Medio Alto, Medio, Medio Bajo, y Bajo, éstos representan el nivel en el que se expone el activo de información de la institución, se detalla en el ANEXO 2.

La explotación de vulnerabilidades de alguno de los activos en la institución presenta procedimientos a seguir para dar solución dentro del área tecnológica, cuando no existen procedimientos o normativas se presenta o dispone acciones a los responsables de las áreas para dar cumplimiento con los objetivos tecnológicos, en la Tabla N° 6 se detalle la definición de cada uno de los niveles de riesgo.

Tabla 6.

Escala del riesgo de tecnología

Nivel del riesgo	Descripción del riesgo y acciones necesarias
Alto	Requiere fuertes medidas correctivas, planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de la directiva.
Medio alto	Requiere vigilancia de la alta directiva con planes de tratamiento implementados y reportados a los jefes de área.
Medio	Requiere acciones correctivas controladas por grupo de manejo de incidentes en periodo de tiempo razonable
Medio bajo	Riesgo aceptable.- administrado por los grupos de incidentes bajo procedimientos normales de control
Bajo	El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo.

Fuente: López & Lala, 2013

Los niveles de aceptación del riesgo por parte de la institución, establece que el nivel Medio alto y Alto son inaceptables y deben tener un tratamiento de forma inmediata ya que la ocurrencia de estos riesgos perjudica la imagen de la institución. De la misma forma los niveles "Medio" – "Bajo" debe tratárselos poniendo mayor control para mitigar el riesgo con el fin de alinearse a los objetivos estratégicos de la institución.

Resultado obtenido del proceso.- Está basado en el resultado de la evaluación de las encuestas las mismas que fueron homologadas con los controles de la ISO 27002 de ésta manera se determina la existencia de monitoreo y controles en el área de tecnología de la Institución.

El resultado de la evaluación permite verificar la existencia de controles e identifica el nivel de madurez tecnológico con respecto a los dominios de la ISO27002, empleando mediciones de acuerdo al CMM de COBIT 4.0, las mismas que están representadas por el siguiente estándar, ver Figura N° 19:

- 0 = **No existente**: no hay procesos de control reconocido.
- 1 = **Inicial / Ad hoc**: La dirección reconoce el problema que debe ser tratado, sin embargo no existen procesos estandarizados.
- 2 = **Repetible pero intuitivo**: Se desarrolla procesos por diferentes personas entendiendo las mismas tareas. No hay comunicación ni entrenamiento formal.
- 3 = **Proceso definido**: Los procesos se definen, documentan y se comunican a través del entrenamiento formal.
- 4 = **Administrados y medibles**: Existe medición y monitoreo sobre cumplimiento de los procedimientos.
- 5 = **Optimizado**: Los procesos se refinan a nivel de buenas prácticas con base en los resultados del mejoramiento continuo.

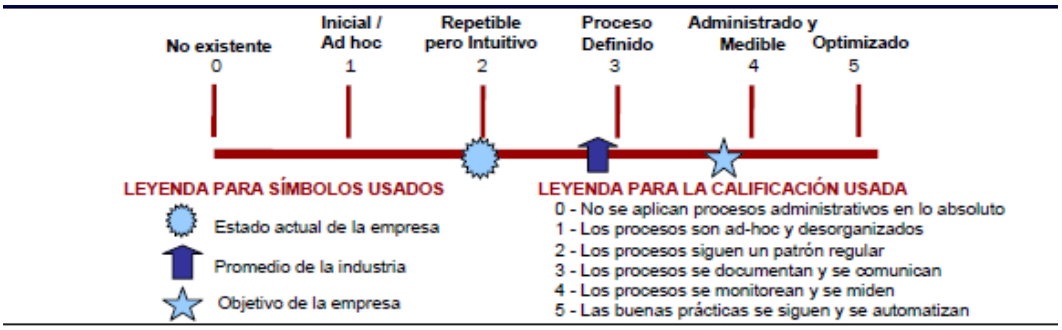

Figura 19, Nivel de madurez CMM de COBIT 4.O

3.7 Levantamiento de Información en las Entidades Municipales.

El levantamiento de información tiene como objetivo examinar a las entidades y/o dependencias municipales Quito para determinar el cumplimiento y utilización de las políticas de tecnología a cargo de la Dirección Metropolitana de Informática; de ésta forma se identifica las políticas, procedimientos que utilizan las dependencias que en su labor diaria.

Para realizar el levantamiento de información se estableció objetivos, tipo de investigación, métodos, técnicas que se va a utilizar en el transcurso del desarrollo

del proyecto, el cual tiene como objetivo determinar resultados a través de las encuestas.

3.8 Estructura Organizacional de la Dirección Metropolitana De Informática

La estructura organizacional de la Dirección Metropolitana de Informática se sustenta en la Resolución Nro. A 010 emitida el 31 de marzo 2011, en la cual orgánicamente dependen de la Administración General del Municipio del Distrito Metropolitano de Quito.

3.8.1 Organigrama Estructural de la Dirección Metropolitana de Informática

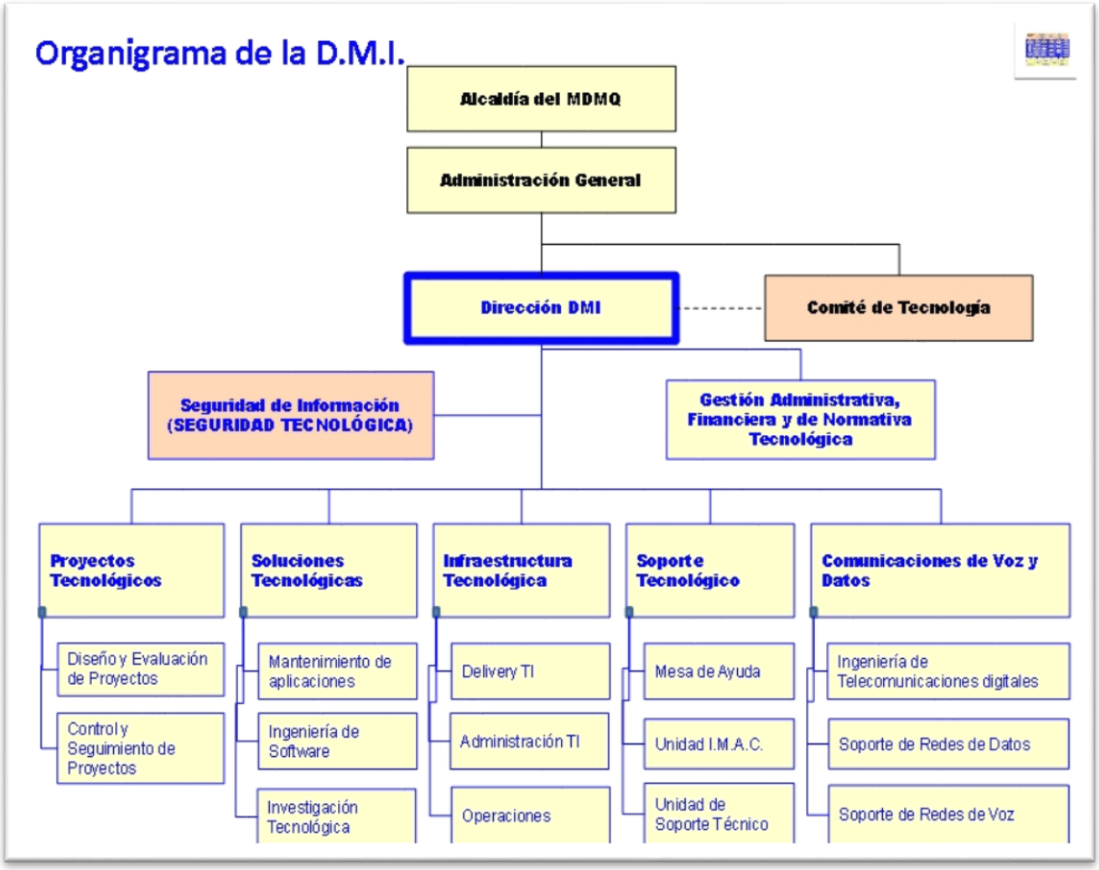

Figura 20. Organigrama Estructural de la DMI

La Dirección Metropolitana de Informática es la entidad que parame triza el uso de los sistemas de comunicación, telecomunicaciones que permiten a los funcionarios o miembros de la institución tener una puerta abierta a los recursos de la información a través de una conexión a Internet. Es por esto que la Dependencia al ser el custodio de los datos y mantener la Seguridad de la Información presenta las Políticas Específicas para el uso de Recursos tecnológicos, de conectividad y la aplicación de estándares tecnológico.

Las políticas establecen reglas, directrices, estándares en cuanto a la aplicación de los recursos tecnológicos (lógicos y físicos) de tal manera que permite establecer un modelo de Gestión Tecnológica la misma que forma parte de la Gestión Institucional del Servicio Público. Ver Figura 21 (Políticas de Gestión Tecnológica DMI, 2011,p.6).

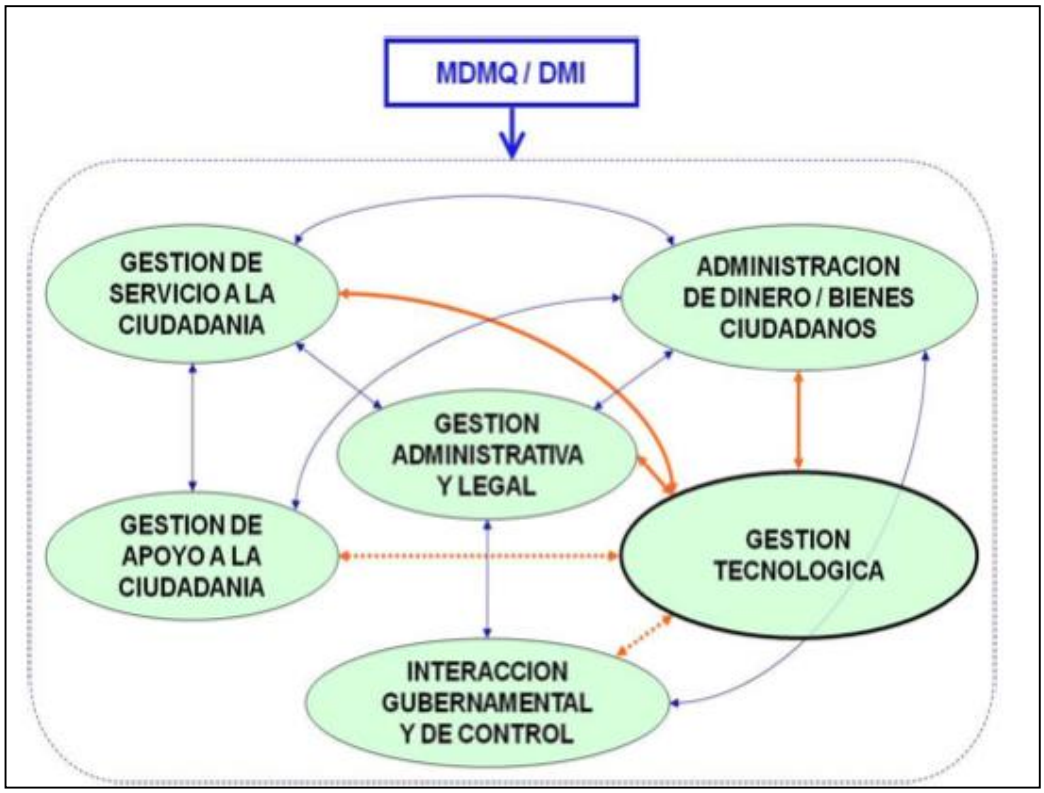

Figura 21. Modelo de Gestión Tecnológica (Políticas de Gestión Tecnológica de la DMI, 2011)

El modelo de Gestión Tecnológica de acuerdo a las Políticas de Gestión Tecnológica de la DMI, está orientado a SERVICIOS DE CALIDAD.

El esquema global de la Gestión Tecnológica que mantiene la Dirección Metropolitana de Informática abarca a los procesos que tiene las áreas (Ingeniería de Soluciones, Redes y Comunicaciones, Soporte Tecnológico, Producción Tecnológica). Ver Figura N° 22, Esquema de la Gestión Tecnológica Orientado a Servicios (Políticas de Gestión Tecnológica DMI, 2011)

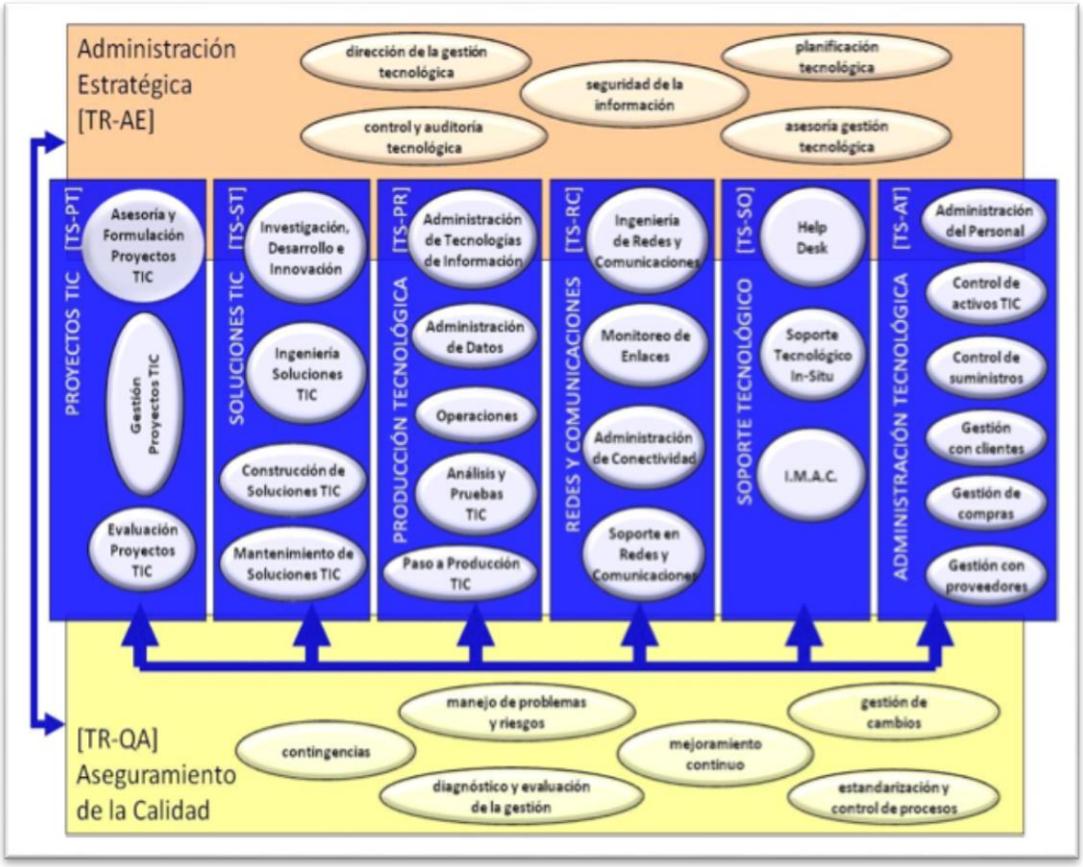

Figura 22. Esquema de la Gestión Tecnológica Orientado a Servicios (Políticas de Gestión Tecnológica DMI, 2011, p.7)

Las políticas de Gestión Tecnológica dentro de su estructura contempla la gestión en las áreas con definiciones procedimentales; las mismas que trabajan en concordancia con lo dispuesto en las Normas de Control Interno del Sector Público de acuerdo a la sección 410 Tecnología de la Información, (Políticas de Gestión Tecnológica de la DMI, 2011)

- **Gestión de Proyectos.-** Determina el análisis, periodicidad y autorización de los anteproyectos y acoplarle en el plan operativo del periodo de gestión.

De la planificación de los proyectos en el cual consideran recursos, costos y tiempos para su cumplimiento.

De la contratación establece directrices para la adquisición de software o soluciones tecnológicas.

Del seguimiento establece la forma para el seguimiento y avance de los proyectos.

Del Cierre establece la forma de realizar el cierre del proyecto.

- **Seguridad Informática.-** Determina el nivel de confidencialidad que debe tener la información a niveles de seguridad física o lógica, establece directrices para la autorización, autenticación, y acceso.
- **Gestión de los recursos informáticos**.- Determina la responsabilidad que deben tener la dependencias municipales respecto al inventario de los recursos informáticos, adquisición de equipos, mantenimiento y control de equipos informáticos.
- **Delitos Informáticos**.- Se basa en lo que establece la Ley de Comercio Electrónico, Firmas y Mensaje de datos.
- **Servicio de Tecnología**.- Determina el uso del recurso por parte del personal de la institución garantizando los objetivos y requerimientos de la institución.
- **De la Calidad**.- Define la calidad como el principal objetivo estratégico institucional que se encuentra a disposición de los usuarios y clientes.

  Establece los principios normativos de calidad de Soluciones Tecnológicas, productos Tecnológicos.

3.9 Tipos de Investigación.

3.9.1 Investigación de Campo.

La investigación a realizarse es con el método Exploratorio, con ello se pretende identificar la situación actual de las instituciones y dependencias. La investigación se va a realizar a los técnicos desconcentrados que se encuentran en las dependencias o

administraciones y para ello se elaboró diferentes encuestas estructurada con opción múltiple y de acompañamiento asistido.

Las encuestas desarrolladas para el área de tecnología es el principal insumo para recopilar información, las mismas que están divididas para las áreas que se menciona a continuación:

- Centro de Atención Tecnológica. ANEXO 1.1
- Producción (Control de Calidad, Base de datos, Soporte). ANEXO 1.3
- Redes. ANEXO 1.4
- Ingeniería de Soluciones. ANEXO 1.2

3.9.2 Investigación Bibliográfica.

La investigación Bibliográfica se consultaron diversas fuentes, tales como: políticas, normativa interna de la DMI, marcos de referencia, sitios web referentes al área de investigación.

3.10 Calculo Muestral.

3.10.1 Ámbito Geográfico.

La investigación será realizada en la Dirección Metropolitana de Informática, Dependencias afines y Administraciones Zonales que forman parte del Municipio de Quito, ya que la ejecución de las políticas tecnológicas se centraliza en la Dirección Metropolitana de Informática (DMI), y se expanden a las dependencias desconcentradas.

3.10.2Sujeto de Análisis.

Las encuestas a realizarse con acompañamiento está direccionada a los técnicos desconcentrados, responsables de mantener la operatividad, integridad, disponibilidad de la información, servicio en las dependencias desconcentradas; de la misma manera a los administradores responsables de precautelar la información.

3.10.3Tamaño de la Muestra.

De acuerdo a la estructura orgánica funcional del Municipio del Distrito Metropolitano de Quito, cuenta actualmente con la Dirección Metropolitana Informática, Secretarias y Administraciones Zonales que se detallan a continuación:

Tabla 7

Encuestas de las Dependencias y Administraciones zonales

Dependencias	Nro. Dependencias	Nro. De encuestas
Secretarías	13	27
Administraciones zonales	9	27
Unidades educativas	5	8
Patronatos	3	9
Policía Metropolitana	1	3
Dirección Metropolitana de Informática	1	30
Ingeniería de Soluciones		
Centro de Atención Tecnológica		
Producción.		
Redes		

Fuente: López & Lala, 2013

Las encuestas se realizaron con acompañamiento en la institución, determinado que el tipo de población es finita equivalente a 31 instituciones municipales, es así que la muestra es igual a la población.

3.11 Herramienta de Investigación.

La recolección de información se desarrolló en base a cuestionarios divididos por áreas de tecnología, para identificar el cumplimiento de cada uno de los objetivos, la encuesta está diseñada para determinar el grado de cumplimiento de las políticas e identificar los posibles riesgos que no han tenido un control adecuado. La encuesta está conformada por tres partes:

3.11.1Introducción y Solicitud de colaboración.

En ésta sección se informa el objetivo que se requiere alcanzar con la recolección de información.

3.11.2Cuerpo de la encuesta.

Las encuestas presentan respuesta de opción múltiple las mismas que representan al grado de confianza y cumplimiento de la política.

Las encuestas se realizaron clasificando de acuerdo a las áreas de tecnología, en base a los criterios definidos en la INEN- ISO/ IEC 27002:2009(Tecnología de la Información- Técnicas de la Seguridad- Código de práctica para la gestión de la Seguridad de la Información), los cuales se encuentran desagregados por la política de Gestión Tecnológica.

- Centro de Atención Tecnológica.
    - Inventario de Usuarios.
    - Niveles de Soporte
    - Actualización de Hardware.
    - Actualización de Software.
    - Acceso a Internet, correo electrónico
    - Mantenimiento de Equipos
    - Inventario de Software y Hardware.
    - Control de Conexión en las redes.
    - Seguridad de los equipos fuera de las instalaciones.
    - Monitoreo
    - Otros
- Infraestructura (Control de Calidad, Base de datos, Soporte)
    - Respaldo de Información
    - Fuga de información.
    - Disponibilidad de Servicio
    - Plan de Contingencia
    - Seguridad en la instalación.

- Versionamiento de aplicativos.
- Procedimientos para cumplimiento de operaciones
- Accesos a Base de datos.
- Actualización de los Sistemas de gestión de base de datos.
- Licenciamiento de Sistema Operativo
- Encriptación de claves.

- Redes.
  - Seguridad perimetral
  - Control de tráfico.
  - Monitoreo de la red.
  - Denegación de Servicio.
  - Acceso no autorizado.
- Ingeniería de Soluciones.
  - Modificación en los aplicativos
  - Derechos de autor
  - Encriptación de claves.
  - Validación de los aplicativos.
  - Accesos al código fuente de los aplicativos

Las dependencias encuestadas se detallan en la Tabla N° 8.

Tabla 8.

Detalle de las dependencias encuestadas

DEPENDENCIAS Y ENTIDADES MUNICIPALES	ENCUESTAS			
	CAT	Redes	Producción	Ing. Soluciones
ADMINISTRACIONES ZONALES				
NORTE (EUGENIO ESPEJO)	X	X	X	
CENTRO (MANUELA SÁENZ)	X	X	X	
QUITUMBE	X	X	X	X
SUR (ELOY ALFARO)	X	X	X	
LA DELICIA (EQUINOCCIO)	X	X	X	

Continúa →

CALDERÓN	X	X	X	
LOS CHILLOS	X	X	X	
TUMBACO	X	X	X	
LA MARISCAL	X	X	X	
UNIDADES MUNICIPALES DE SALUD				
NORTE	X	X	X	
CENTRO	X	X	X	
SUR	X	X	X	X
SECRETARIAS	X	X	X	X
SECRETARIA DE TERRITORIO, HABITAD Y VIVIENDA	X			
SECRETARIA DE EDUCACIÓN, RECREACIÓN Y DEPORTE	X	X		X
SECRETARIA DE SEGURIDAD Y GOBERNABILIDAD	X			
SECRETARIA DEL AMBIENTE	X	X	X	
SECRETARIA DE SALUD	X	X	X	X
SECRETARIA DE DESARROLLO PRODUCTIVO	X			
SECRETARIA DE MOVILIDAD	X	X		
DEPENDENCIAS				
DIRECCIÓN METROPOLITANA DE INFORMÁTICA	X	X	X	X
UNIDADES EDUCATIVAS				
FERNÁNDEZ MADRID	X	X	X	
UNIDAD QUITUMBE	X	X	X	
SUCRE	X	X	X	
ESPEJO	X	X	X	
COLEGIO BENALCÁZAR	X	X	X	
ESCUELA SAN FRANCISCO DE QUITO	X	X	X	
OTRAS				
POLICÍA METROPOLITANA	X	X	X	X
AGENCIA METROPOLITANA DE CONTROL	X	X	X	
AGENCIA DE COMERCIALIZACIÓN	X	X	X	

Fuente: López & Lala, 2013

3.12 Datos de Clasificación.

3.12.1 Identificación de Activos.

La Dirección Metropolitana de Informática considera a los activos como los recursos de los sistemas de Información los cuales se encuentran directamente relacionados con el objetivo que la Organización referente al cumplimiento de metas

propuestas por la Alta Dirección; de la existencia del tipo de activo, las amenazas y los controles pueden variar (aumentar o disminuir).

3.12.2 Caracterización de los activos.

Los activos se determinan pos las características que lo definen:

- Código o nombre, procedente del inventario
- Tipo de activo.
- Servicios Soportados.
- Datos o información comprendida.
- Unidad responsable.
- Ubicación geográfica.

La identificación de las características de los activos hace que puedan ser agrupados de la siguiente manera:

- Equipos Informáticos (Información/Servicios)
- Redes de Comunicaciones.
- Instalaciones.
- Datos / Información

Equipos Informáticos.- Representa a los bienes físicos, utilizados para dar soporte directa o indirecta de los servicios que presta la organización, pueden ser soporte de ejecución de las aplicaciones informáticas o transporte de datos.

Redes de comunicaciones.- Denominada a la instalación dedicada a servicios de comunicaciones propios, pero determinados como medio de transporte que llevan datos de un sitio a otro (Antenas, canal de comunicación).

Instalaciones.- Lugares físicos donde están ubicados en su tiempo, para lo cual se debe tener presente a los activos el caso de la institución el activo es la información (datos).

Datos / Información.- Representa a las aplicaciones que gestionan, analizan y transforman los datos para prestar servicios a la institución.

Los activos más relevantes en la institución son los datos y servicios, para lo cual, su funcionalidad depende de otros activos base los mismos que pueden ser

equipos, comunicaciones o personal, la ejecución de una amenaza en un activo superior tiene como consecuencia un perjuicio sobre activo inferior.

Se puede interpretar que los activos inferiores son los cimientos en los que se apoya la seguridad del activo superior por tal motivo a la organización se la representa como una pirámide de soporte de la información, en el cual los niveles de superiores dependen de los inferiores: Ver Figura N° 23.

- Nivel 1.- Representan a los activos requeridos para garantizar la capa de entorno físico.
- Nivel 2.- Representa a los sistemas de información tales como (hardware, software, datos, cintas, discos).
- Nivel 3.- Objetivos que presenta la institución para mantener en el ámbito del negocio.

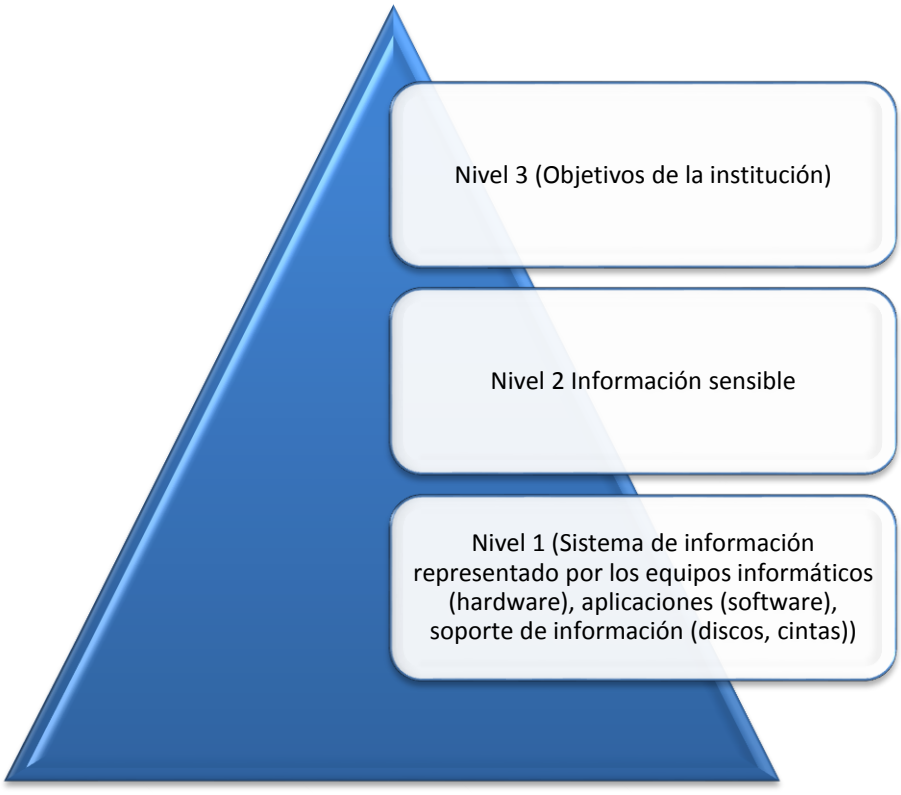

Figura 23. Niveles de activos de Información, (López & Lala, 2013)

3.12.3 Inventario de activos

La estructura de los activos identificados en la DMI y las dependencias desconcentradas se describe a continuación:

Nivel 1: Activos relacionados con el soporte de la información (entorno físico, mobiliarias, personal, etc), ver Tabla 9.

- **Instalaciones:** Identifica los centros de cómputo, donde se encuentran los sistemas de información.
- **Soporte.-** Equipos relacionados con UPS, aire acondicionado, requeridos para garantizar el funcionamiento del centro de cómputo.

Red de comunicaciones.- instalaciones dedicadas a servicios de comunicaciones de las administraciones zonales.

Tabla 9.

Activos de información, Nivel 1

Activos	Valor	Tipo	Estado
Servicios	Servicio de pago en línea de los impuestos por medio de instituciones financieras (Teller, SAO, PATENTES)	$40.000.000	Intangible
Datos / Información	Bases de datos en oracle spacial, oracle, sql server, reglamentos código fuente de los sistemas (SIREC-Q Espacial)	$9.000.000	Intangible
Aplicaciones	Aplicativos de recaudación municipal, catastral, seguridad(SIREC-Q, SGCT,SLUM, TRANSFERENCIA DE DOMINIO, IRM)	$ 300.00	Intangible
Equipos informáticos	Servidores, switch, router , firewall	$5.000.000	Tangible
Redes de Comunicaciones	DispositiVos comunicación de red local, telefónica, inalámbrica	$ 800.00	Tangible
Soporte de información	Discos duros, storage	$1.600.000	Tangible
Instalaciones	Data center de la DMI y dependencias desconcentradas	$7.600.000	Tangible
Equipamiento auxiliar	Cintas de almacenamiento	$ 400.00	Tangible
Total		**$64.700.000**	

Fuente: López & Lala, 2013

Nivel 2.- Sistema de Información definidos como los equipos informáticos, servidores, dispositivos de seguridad, dispositivos de comunicaciones, soporte de información (cintas), acceso, aplicaciones, base de datos de la DMI.

Tabla 10.

Activos de Información tecnológico de la DMI

Valoración cualitativa y Cuantitativa de los activos de Información del MDMQ		
Escala Cualitativa	**Cuantitativa**	**Descripción**
Alto	1	Más de $32.000.001 mensuales
Medio Alto	2	de $ 24.000.001 - $32.000.000
Medio	3	de $16.000.0001 - $24.000.000
Medio Bajo	4	Hasta $16.000.001
Bajo	5	Hasta $800.000

Fuente: López & Lala, 2013

3.13 Análisis de Vulnerabilidades y Amenazas en las Áreas de Tecnología.

De acuerdo a la ISO 27002, las amenazas son eventos imprevistos con el objetivo de causar daños, por lo tanto las amenazas explotan vulnerabilidades que se presentan en cualquier ámbito del área de tecnología.

La determinación de la valoración de las vulnerabilidades encontradas a través de las encuestas se realiza de acuerdo a la tabla N. 3 (Valoración de Probabilidad, Capítulo II), la misma que se basa en la norma de la (ISO/IEC27001,numeral4.1).

3.14.1 Área de Centro de Atención Tecnológico

De acuerdo a las encuestas realizadas a los entrevistados o identificados durante las visitas a sitio en el departamento del CAT (Centro de Atención Tecnológica) de la Dirección Metropolitana de Informática, luego de la tabulación se identificaron las siguientes vulnerabilidades las mismas que se consolidan en el ANEXO 3.3 y se detallan en la tabla 11. *Vulnerabilidades detectadas del área de CAT*, que representan el incumplimiento a la política de gestión tecnológica encontrándose en las siguientes zonas de riesgo:

Tabla 11.

Vulnerabilidades detectadas del área de CAT.

	Vulnerabilidad
Zona inaceptable	Pérdidas de activos físicos y lógicos
Zona moderada	Falta de control en la determinación de IP públicas
	Ausencia de documentación para actualización del Hardware
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de documentación para actualización e inventario del Hardware
	Ausencia de un eficiente control de cambios en la configuración y adquisición de hardware
	Ausencia de promoción y repositorio de manuales técnicas
Zona tolerable	Incumplimiento en el mantenimiento del cableado
	Ausencia de Inventario de la parte interna del equipo
	Ausencia de políticas para el uso correcto de internet y mensajería
	Ausencia de acuerdos de niveles de servicio, o insuficiencia de los mismos
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Existencia de código malicioso (virus, troyano)
Zona aceptable	Ausencia de documentación para actualización de manuales técnicos

Fuente: López & Lala, 2013, anexo 3.3

Las vulnerabilidades identificados son: inexistencia de controles que apoyen en la gestión de tecnología, por lo tanto, la ausencia de controles ha provocado que el personal realice las actividades de forma intuitiva generando que no exista procedimientos que permitan la actualización e inventario de hardware y software, desconocimiento de la existencia de manuales técnicos para el personal técnico, procedimientos que determinen los acuerdos de niveles de servicio, procedimientos de acceso para la activación y desactivación de usuarios en las diferentes plataformas tales como (DA, VPN, acceso etc), ausencia de controles que permitan realizar cambios en la configuración y adquisición de hardware generando pérdidas en los componentes de los equipos o dispositivos, etc.

A continuación se presentan de forma estadística el análisis a los resultados obtenidos de las vulnerabilidades del área de Centro de Atención Tecnológica, ver figura 24.

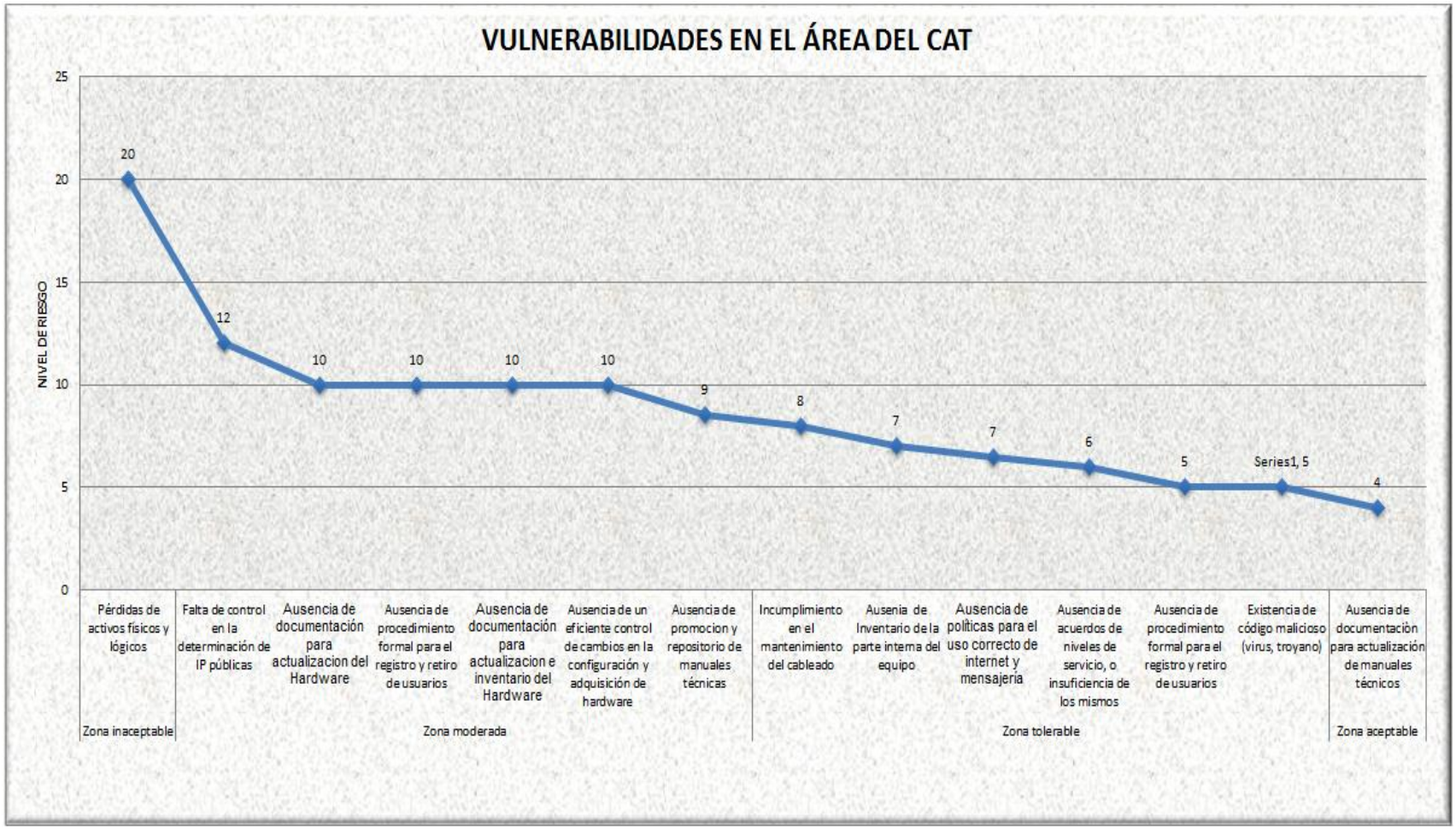

Figura 24. Cuadro estadístico de las Vulnerabilidades detectadas en el área del CAT

Las amenazas detectadas a las vulnerabilidades encontradas en el Área del CAT de acuerdo al Anexo D de la norma NTC-ISO/IEC 27005 se detallan a continuación: ver Tabla N° 12

Tabla 12

Cuadro estadístico de las Amenazas en el área de CAT, ANEXO

	Amenazas
Zona inaceptable	Destrucción de equipos o de medios.
	Ausencia de procedimiento formal para el registro y retiro de usuarios
Zona moderada	Falta de actualizaciones al Software
	Acceso forzado al sistema
	Error en el uso
	Abuso de derechos
Zona tolerable	Pérdida de equipos
	Incumplimiento en el mantenimiento del sistema de información
	Falta de difusion de los conocimiento
	Uso no autorizado del equipo
Zona Aceptable	Falta de actualizaciones al Hardware

Fuente: López & Lala, 2013, anexo 3.4

Las zonas de riesgo se encuentran agrupados por riesgo inaceptable, moderado, tolerable y aceptable, para lo cual todas las amenazas encontradas deben ser tomadas en cuenta para implementar controles, en mayor grado de importancia al riesgo moderado e inaceptable el cual afecta directamente a los activos de información.

A continuación se presentan estadísticas de análisis a los resultados obtenidos de las amenazas detectadas en las vulnerabilidades del área de Centro de Atención Tecnológica, ver figura 25.

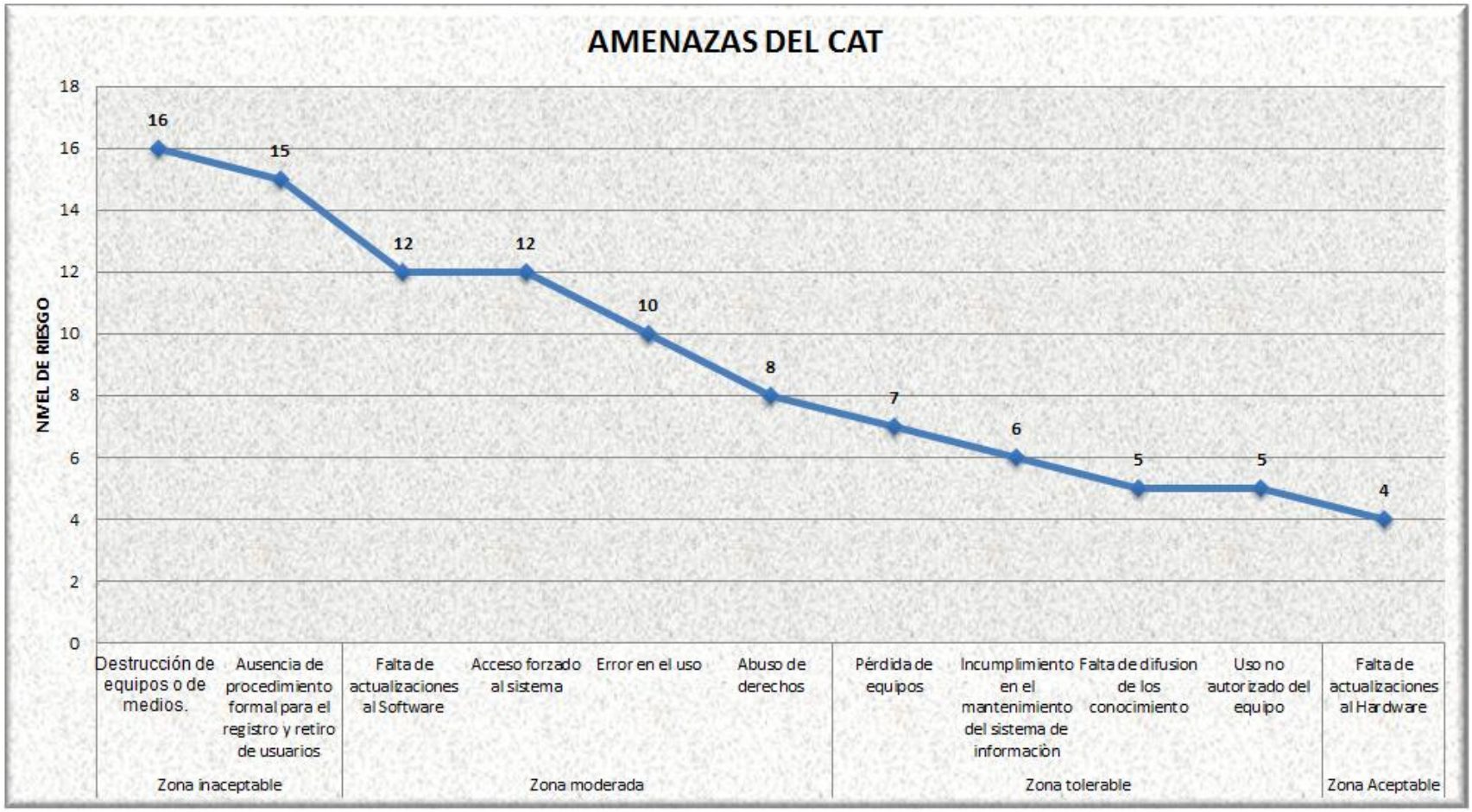

Figura 25. Amenazas detectas en el CAT

3.14.2 Área de Producción

De la misma forma al realizar las encuestas a los entrevistados o identificados durante las visitas a sitio en el departamento de Producción de la Dirección Metropolitana de Informática se registraron vulnerabilidades las mismas que se consolidan en el anexo 4.3 y se detallan en la tabla 13. *Vulnerabilidades detectadas del área de Producción*, que representan el incumplimiento a la política de gestión tecnológica encontrándose en las siguientes zonas de riesgo:

Tabla 13.

Vulnerabilidades detectadas del área de Producción.

Zona de Riesgo	**Vulnerabilidad**
Zona inaceptable	Ausencia de plan de continuidad (sitio alterno)
	Ausencia de documentación para actualización e inventario del Hardware
	Ausencia de auditorías (supervisiones) regulares
Zona Moderada	Ausencia de respaldo de información
	Ausencia de bitácoras o registro de las claves entregadas
	Ausencia de control de cambios en los aplicativos
	Ausencia de respaldo de las bases de datos
	Ausencia de mecanismos de autorización de acceso y carda de datos a las Bases de datos
	Ausencia de respaldo de la configuración de la virtualización
Zona Tolerable	Ausencia de procedimientos para disponibilidad de servicio
	Ausencia de procedimientos para el ingreso de áreas sensibles
	Ausencia de documentación para la actualización y pruebas del Software
	Ausencia de procedimientos de seguridad que controlen la fuga de información
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
	Ausencia de procedimientos seguridad para el control de la clasificación de información

Continúa →

	Almacenamiento sin protección
	Ausencia de disponibilidad de servicio
	Tabla de contraseña sin protección
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de promoción de manuales técnicas
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de documentación para mantener la seguridad en el suministro de electricidad
	Ausencia de procedimientos para proteger los sistemas operativos
Zona aceptable	Ausencia de protección de los backup
	Ausencia de procedimiento para el registro de actividades del centro de computo
	Software nuevo o inmaduro

Fuente: López & Lala, 2013, anexo 4.3

De acuerdo a las encuestas realizadas a los jefes de área se detectó que el área de Producción es el área de tecnología más crítica ya que se encuentran el control de mando de servidores, bases de datos, versionamiento de los aplicativos que maneja la institución diariamente, en la cual se identificaron vulnerabilidades con alto riesgo de ocurrencia que afectan a los objetivos planteados por la institución, por lo tanto, la ausencia de controles o falta de definiciones en la política de gestión ha generado que el personal a cargo realice actividades sin procedimientos de manera intuitiva provocando mal versionamiento en los aplicativos, falta de disponibilidad en los servicios, daños en los componentes físicos de los servidores, control y monitoreo del respaldo de las bases de datos, error en las actividades que se realiza en el centro de cómputo, inexistencia en el plan de continuidad (sitio alterno), falta de procedimientos formales la revisión (supervisión) y autorización de los derechos de acceso, etc.

A continuación se presentan estadísticas de análisis a los resultados obtenidos de las vulnerabilidades del área de Producción, ver Figura N° 26.

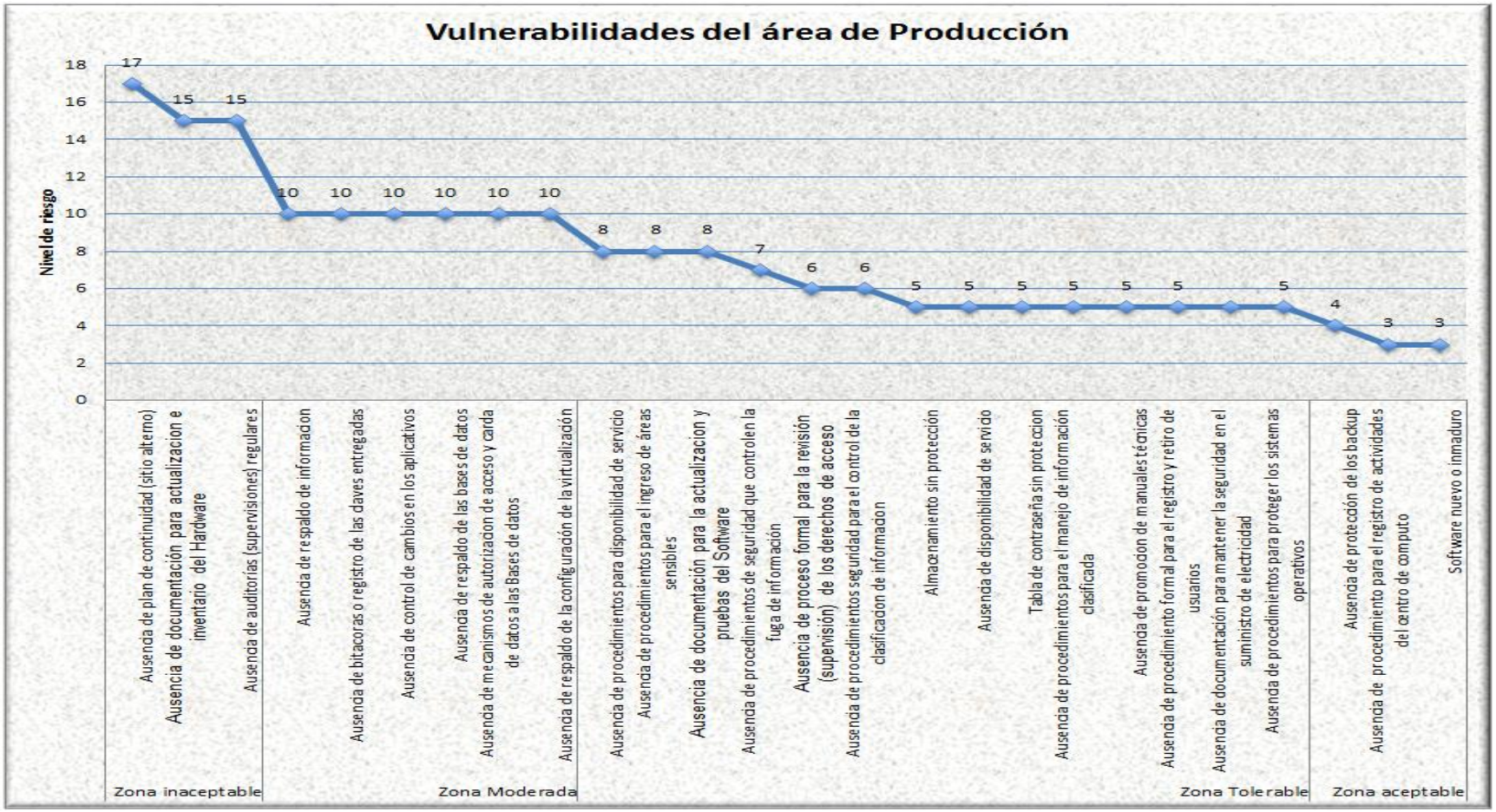

Figura 26. Vulnerabilidades del Área de Producción

Las amenazas más representativas en las vulnerabilidades encontradas del área de Producción se detallan en la Tabla N| 14, de acuerdo al Anexo D de la norma NTC-ISO/IEC 27005.

Tabla 14.

Amenazas detectadas del área de Producción.

	AMENAZAS
Zona inaceptable	Falta de actualizaciones al Hardware
	Falla en los sistemas
Zona Moderada	Abuso de derechos
	Falta de actualizaciones al Software
	Pérdida de las bases de datos
	Hurto de medios o documentos
	Perdida de la configuración de virtualización
	Mal funcionamiento del software(aplicativo)
	Ingreso de persona no autorizado
Zona Tolerable	Manipulación de los equipos por personal no autorizado
	Subir bases de datos con errores
	Pérdida de información
	Uso no autorizado de la información
	error en el uso
	Falta de difusión de los conocimiento
	No existe disponibilidad en los servicios de la institución.
	corrupción de datos, inexistencia de encriptación
Zona aceptable	Ausencia de procedimiento formal para el registro y retiro de usuarios
	mal funcionamiento del software
	Actividades no autorizadas

Fuente: López & Lala, 2013, anexo 4.4

Las amenazas detectadas en el área de Producción están representadas por zonas de riesgo y se encuentran agrupados por riesgo inaceptables, moderadas los mismos que representa a amenazas con alto riesgo de los cuales no existen controles y cuando ocurre los administradores o encargados dan solución implementando parches tecnológicos que en ocasiones afectan a otros servicios y se vuelva una cola de riesgos por falta de procedimientos en autorización de accesos, uso no autorizado de la información, perdida de la información de base de datos, falta de revisión en el monitoreo de los componentes de los servidores, desconocimiento en el mapeo de servidores. A continuación se presentan estadísticas de las amenazas basadas en las vulnerabilidades del área de Producción, ver figura 27.

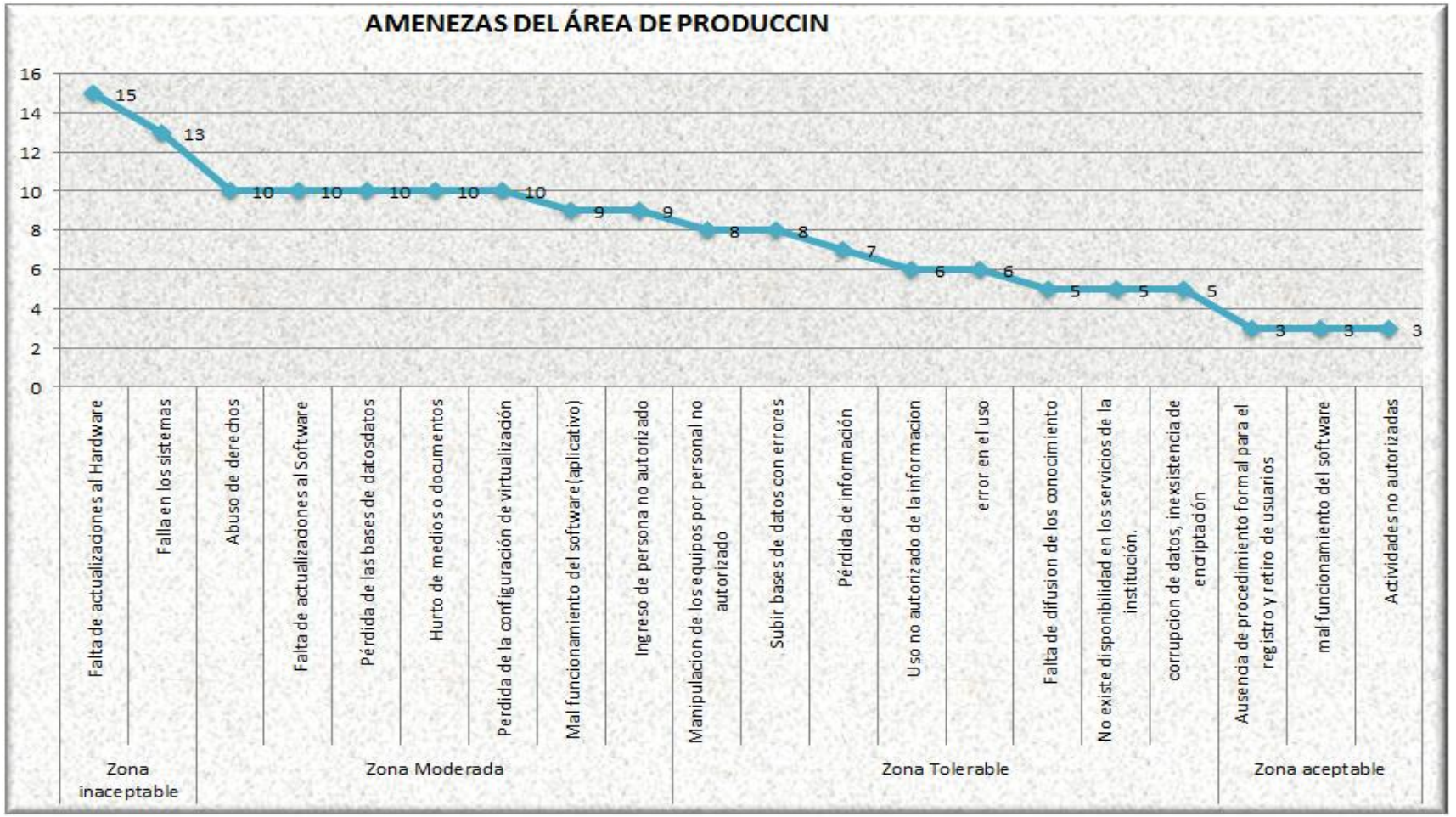

Figura 27. Amenazas encontradas en el área de Producción

3.14.3 Área de Ingeniería de Soluciones

Las vulnerabilidades encontradas en el departamento de Ingeniería de Soluciones identificados durante las visitas se encuentran consolidadas en el ANEXO 5.3 y se detallan en la Tabla N° 15. Vulnerabilidades detectadas del área de Ingeniería de *Soluciones*, que representan el incumplimiento a la política de gestión tecnológica encontrándose en las siguientes zonas de riesgo:

Tabla 15.

Vulnerabilidades detectadas del área de Ingeniería de Soluciones.

	Vulnerabilidad
ZONA INACEPTABLE	Inexistencia de procedimiento y proceso para rendimiento de software
	Incumplimiento en el mantenimiento de los SI
	Ausencia de procedimientos de control de cambios
ZONA MODERADA	Ausencia de procedimiento de aceptación del software
	Ausencia de promoción de manuales técnicas
	Inexistencia de procedimiento para tener los derechos de autor
	Ausencia de procedimiento para la encriptación de información
ZONA TOLERABLE	Ausencia de procedimiento de para desarrollo de software
	Ausencia de procedimiento de para la arquitectura de software
	Ausencia de mecanismos de identificación y autentificación

Fuente: López & Lala, 2013, anexo 5.3

El área de Ingeniería de Soluciones se encuentran entre las áreas críticas puesto que entre las actividades a desarrollarse es la de crear y mantener el ciclo de vida de un sistema en los cuales se encuentra la lógica de proceso, cálculo requerido para el core de la institución, sin embargo, no presenta controles de seguridad y se han identificado vulnerabilidades constantes tales como: ausencia de procedimientos para la encriptación de información, ausencia de procedimientos para el desarrollo de software, ausencia de mecanismos de identificación y autenticación, ausencia de encriptación del código fuente, etc.

A continuación se presentan estadísticas de análisis a los resultados obtenidos de las vulnerabilidades del área de Ingeniería de Soluciones, ver figura 28.

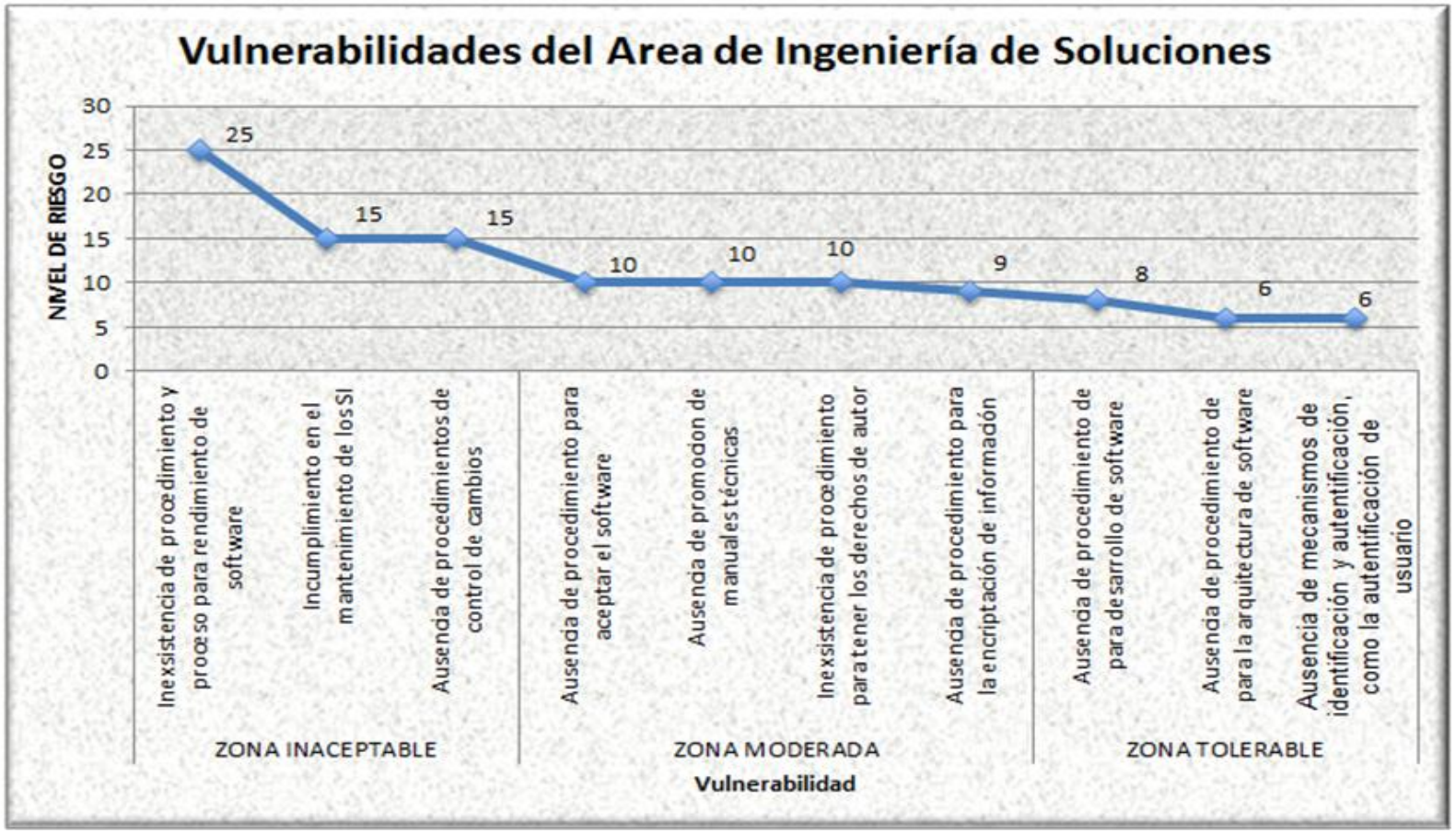

Figura 28, Vulnerabilidades detectadas del área de Ingeniería de Soluciones

Las amenazas más representativas en las vulnerabilidades encontradas del área de Ingeniería de Soluciones se detallan en la Tabla N 16, de acuerdo al Anexo D de la norma NTC-ISO/IEC 27005; la información se encuentra consolidada en el ANEXO 5.4.

Tabla 16.

Amenazas detectadas del área de Ing. de Soluciones, anexo 5.

AMENAZAS	
ZONA INACEPTABLE	Falta de difusión de los conocimiento
	Mal funcionamiento del software
	Abuso de derechos
ZONA TOLERABLE	Falsificación de derechos

Fuente: López & Lala, 2013, anexo 5.4

Las amenazas detectadas en el área de Ingeniería de Soluciones están representada por zonas de riesgo y están agrupadas por riesgo inaceptables, moderadas los mismos que representa a amenazas con alto riesgo de los cuales no existen controles puesto que el personal actúa en el momento de la ocurrencia realizando cambios al aplicativo sin realizar pruebas de stress para verificar el rendimiento del aplicativo y ocasiona un mal funcionamiento del software, no existe encriptación del código fuente adquirido o generado lo que implica un gran riesgo porque existe abuso de derechos, la falta de difusión al personal nuevo que ingresa al área con respecto a conocer la arquitectura de software perjudica porque el personal pierde tiempo creando nuevos componente ya existentes para el desarrollo de software.

A continuación se presentan estadísticas de análisis a los resultados obtenidos de las amenazas detectadas en las vulnerabilidades del área de Ingeniería de Soluciones, ver figura 29

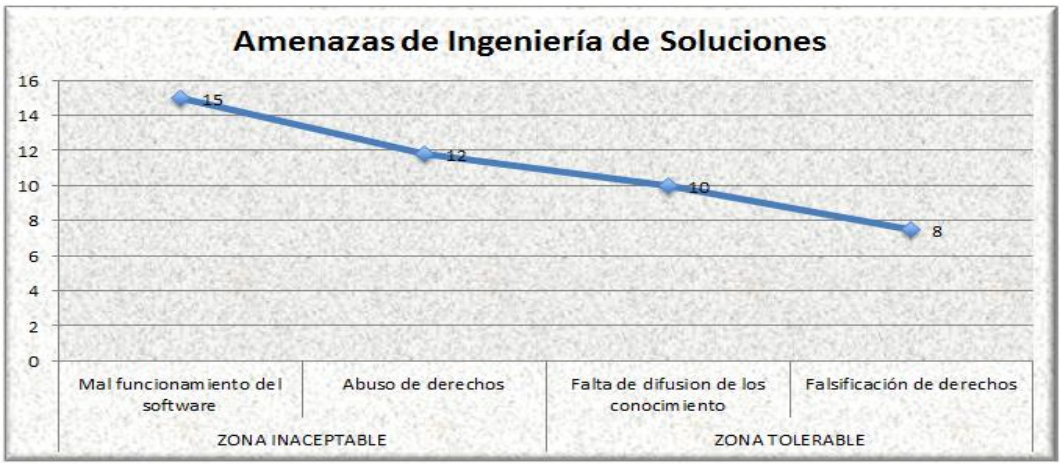

Figura 29. Amenazas detectadas del área de Ing. de Soluciones, anexo 5.

3.14.4 Área de Redes

Las vulnerabilidades encontradas en el departamento de Redes identificados durante las visitas se encuentran consolidadas en el anexo 6 y se detallan en la tabla N 17. Vulnerabilidades detectadas del área de Redes, que representan el incumplimiento a la política de gestión tecnológica encontrándose en las siguientes zonas de riesgo:

Esta información está consolida en el anexo 6.3 y se detalla en la tabla N 17, se registran las vulnerabilidades referenciadas a los entrevistados o identificados durante las visitas a sitio al área de Redes.

Tabla 17.

Vulnerabilidades detectadas del área de Redes

Zona de riesgo	Vulnerabilidad
ZONA INACEPTABLE	Falta de control en la depuración de IP públicas
	Contraseñas sin protección dispositivos de seguridad perimetral y de red
	Ausencia de cambio regulares en las Contraseñas de los dispositivos de seguridad perimetral y de red
	Ausencia de procedimientos para mantener la seguridad de los medios físicos en movimiento.

Continúa →

ZONA MODERADA	Ausencia de procedimientos para administración de incidentes
	Ausencia de procedimientos para la recolección de evidencia de los incidentes de los SI
	Ausencia de procedimientos que detallen debilidades de seguridad de incidentes
	Ausencia de promoción de manuales técnicas
	Gestión inadecuado de la red (tolerancia a fallas en el enrutamiento)
ZONA TOLERABLE	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de información
	Ausencia de procedimientos para depuración de IP en la institución
	Ausencia de respaldo de configuración de los dispositivos de seguridad perimetral y de red
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Respuesta inadecuada de mantenimiento de servicio en el SI
	Ausencia de procedimientos para que realicen intercambio de información entre dependencias
	Inexistencia de acuerdos de intercambio de información
	Respuesta inadecuada de mantenimiento de servicio en el SI

Fuente: López & Lala, 2013, anexo 6.3

Las Vulnerabilidades encontradas en el área de Redes es que no existe un cambio de contraseñas de forma periódica, no existe procedimientos para mantener la seguridad de los medios físicos en movimiento, no existe un procedimiento para la administración de incidentes generando que en cualquier momento exista un ataque externo que interrumpa la disponibilidad de los servicios que brinda diariamente la institución, etc.

A continuación se presentan estadísticas de análisis a los resultados obtenidos de las vulnerabilidades del área de Redes, ver figura 30

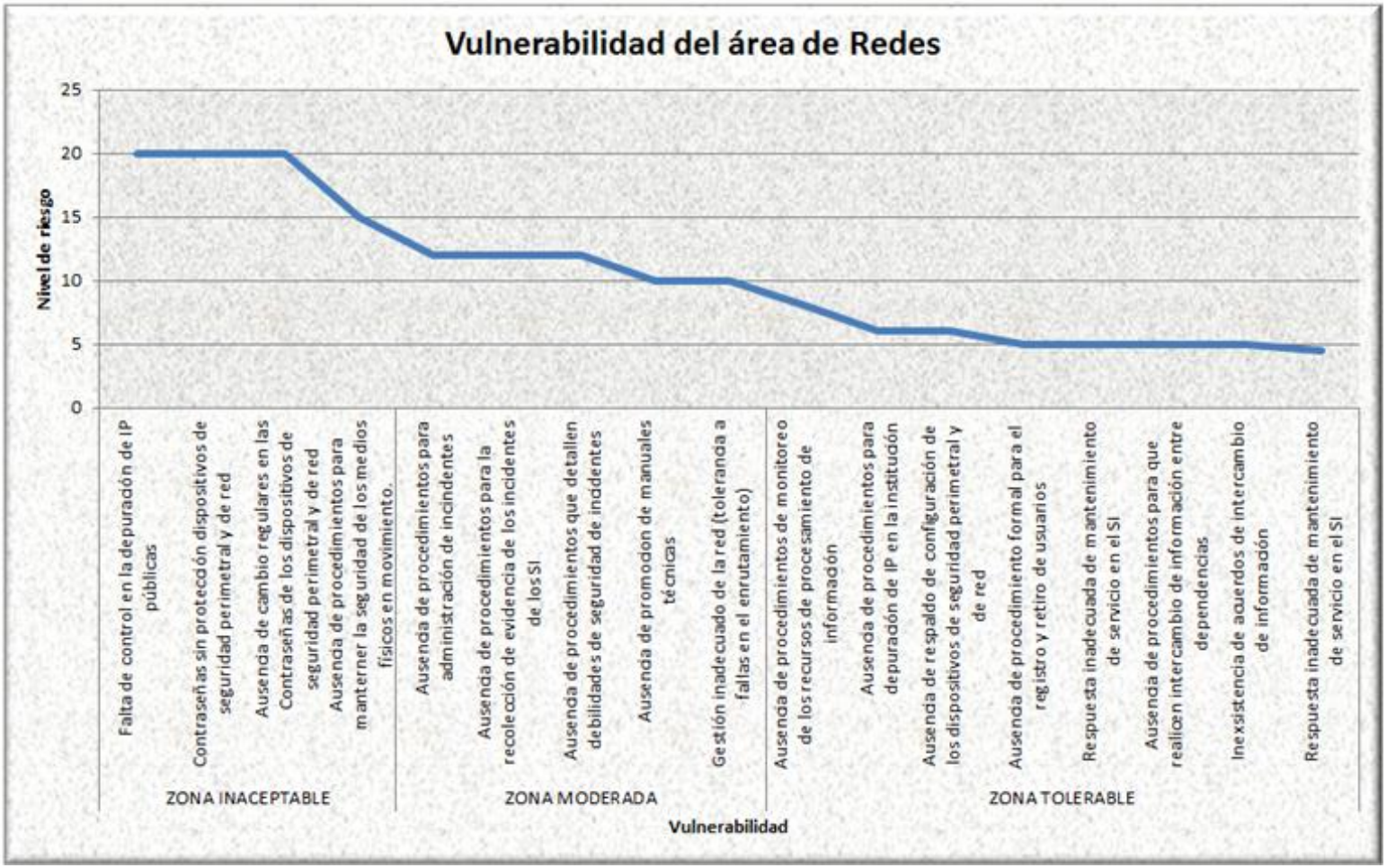

Figura 30. Vulnerabilidades detectadas del área de Redes.

Las amenazas más representativas encontradas en las vulnerabilidades en el área de Redes y de acuerdo al Anexo D de la norma NTC-ISO/IEC 27005 se detallan los siguientes: ver tabla 18

Tabla 18.

Amenazas detectadas del área de Redes.

	Amenazas
Zona inaceptable	Falsificación de derechos
	Espionaje remoto, abuso de derechos.
	Abuso de derechos
Zona moderada	Falta de difusión de los conocimiento
	Saturación del sistema de información
Zona tolerable	Pérdida de información para configurar dispositivos
	Incumplimiento en el mantenimiento de SI
	Abuso de derechos, confidencialidad
	Abuso indebido de información
	Espionaje remoto
	Uso no autorizado a la red

Fuente: López & Lala, 2013, anexo 6.4

A continuación se presentan estadísticas de análisis a los resultados obtenidos de las amenazas detectadas en las vulnerabilidades del área de Redes, ver figura 31.

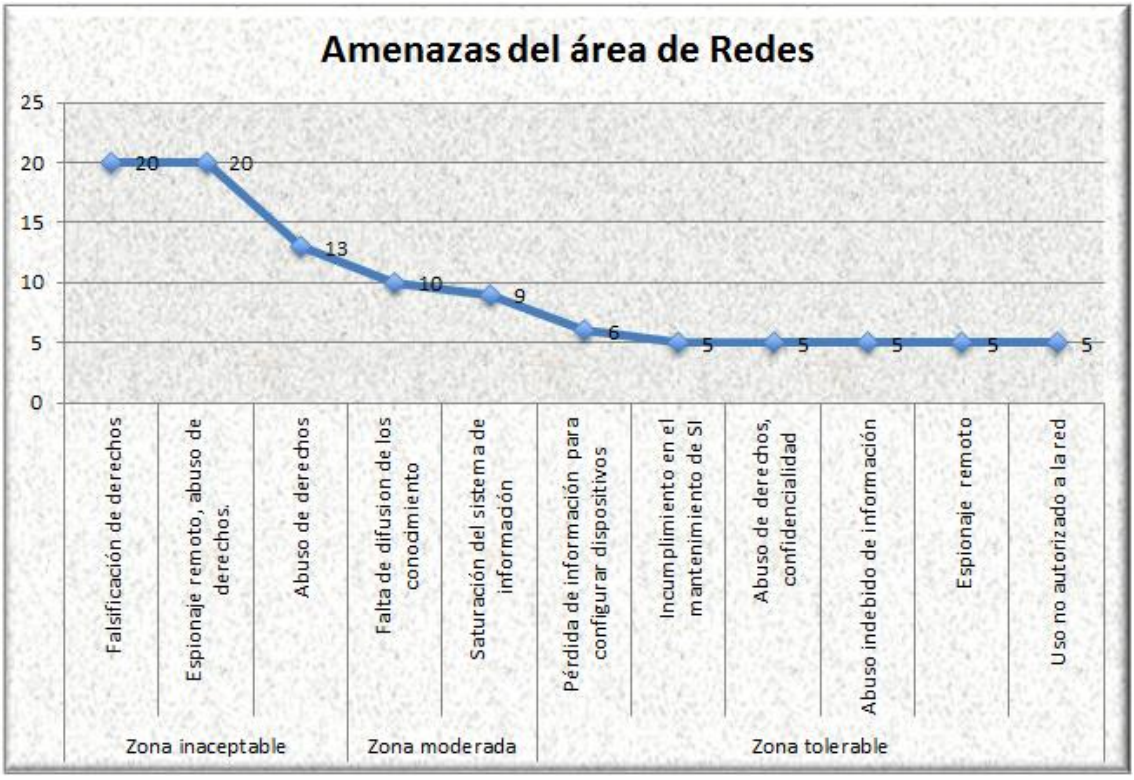

Figura 31. Amenazas detectadas del área de Redes, (López & Lala, 2013), anexo 6.4

3.14 Comparación de cumplimiento de controles

Una vez homologada los controles de la ISO 27002 con los controles que presenta actualmente la institución a través de las políticas de gestión tecnológica, se ha realizado el análisis de comparación en el cumplimiento de las políticas entre la Dirección Metropolitana Informática y las dependencias desconcentradas de la institución. La comparación de cumplimiento se realizó por áreas de tecnología: Producción, Ing. Soluciones, CAT, Redes; a continuación se presentan cuadros estadísticos en los cuales se detalle el nivel de cumplimiento entre la entidad de Control DMI y las dependencias desconcentradas.

3.14.1 Cumplimiento de Controles del CAT VS Áreas desconcentradas

En la Figura N 32, se puede identificar que de parte del CAT existe un mayor cumplimiento de los controles con respecto a la gestión y por ende las dependencias desconcentradas mantienen el mismo lineamiento que el ente rector en la mayoría de

los controles, dejando a un lado los controles de la ISO 27002 que involucran a la seguridad de la información ANEXO 3.2.

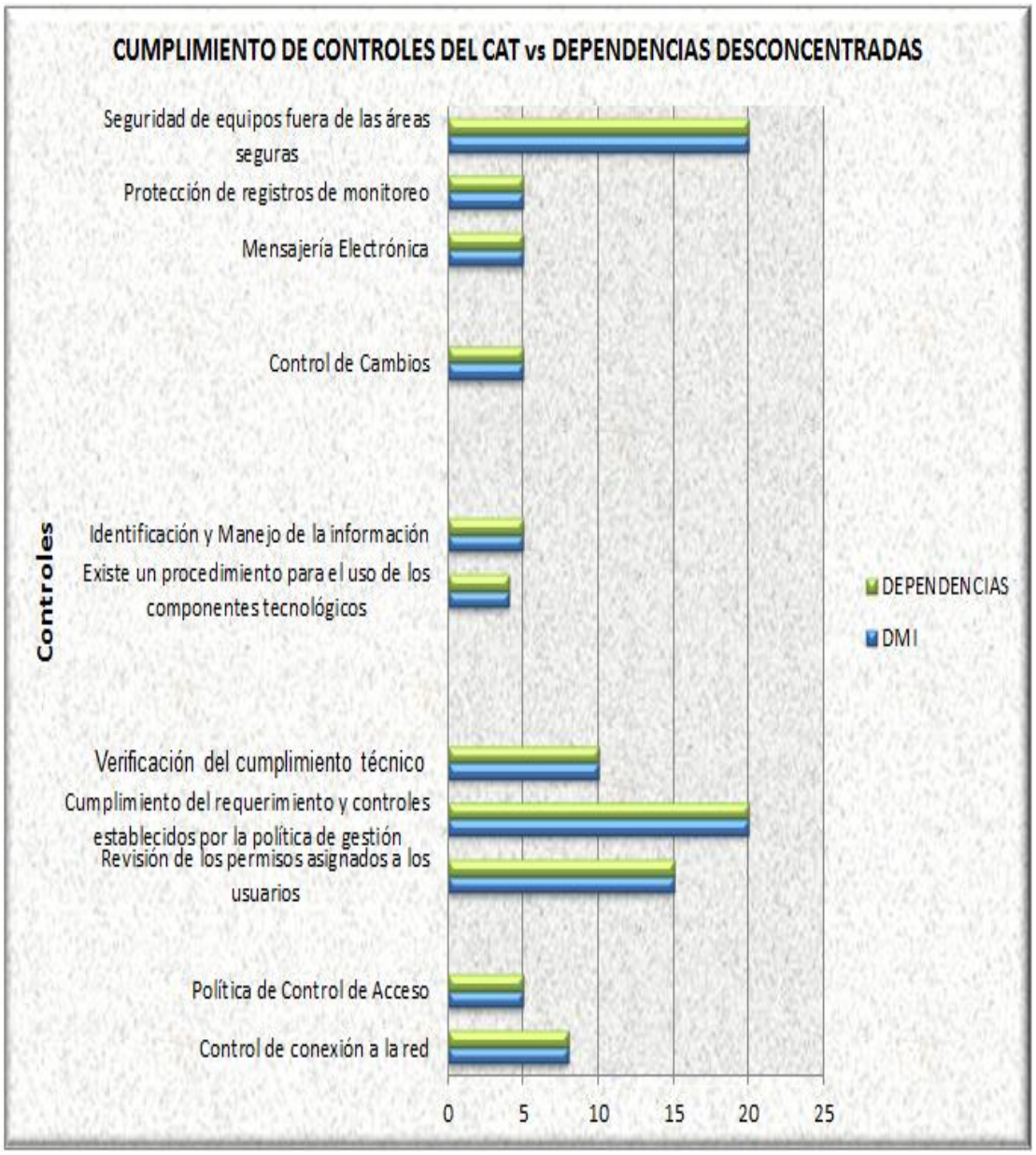

Figura 32. Amenazas detectadas del área de Redes, (López & Lala, 2013)

3.14.1 Cumplimiento de controles de Redes y áreas desconcentradas

En el gráfico se puede apreciar que el área de redes de la DMI, se apega en un grado medio el apego a las normas ISO 27002, dejando abandonado los controles de seguridad mientras que las Dependencias desconcentradas en su mayoría desconocen la existencia de políticas de gestión y actúan de acuerdo a iniciativa propia.

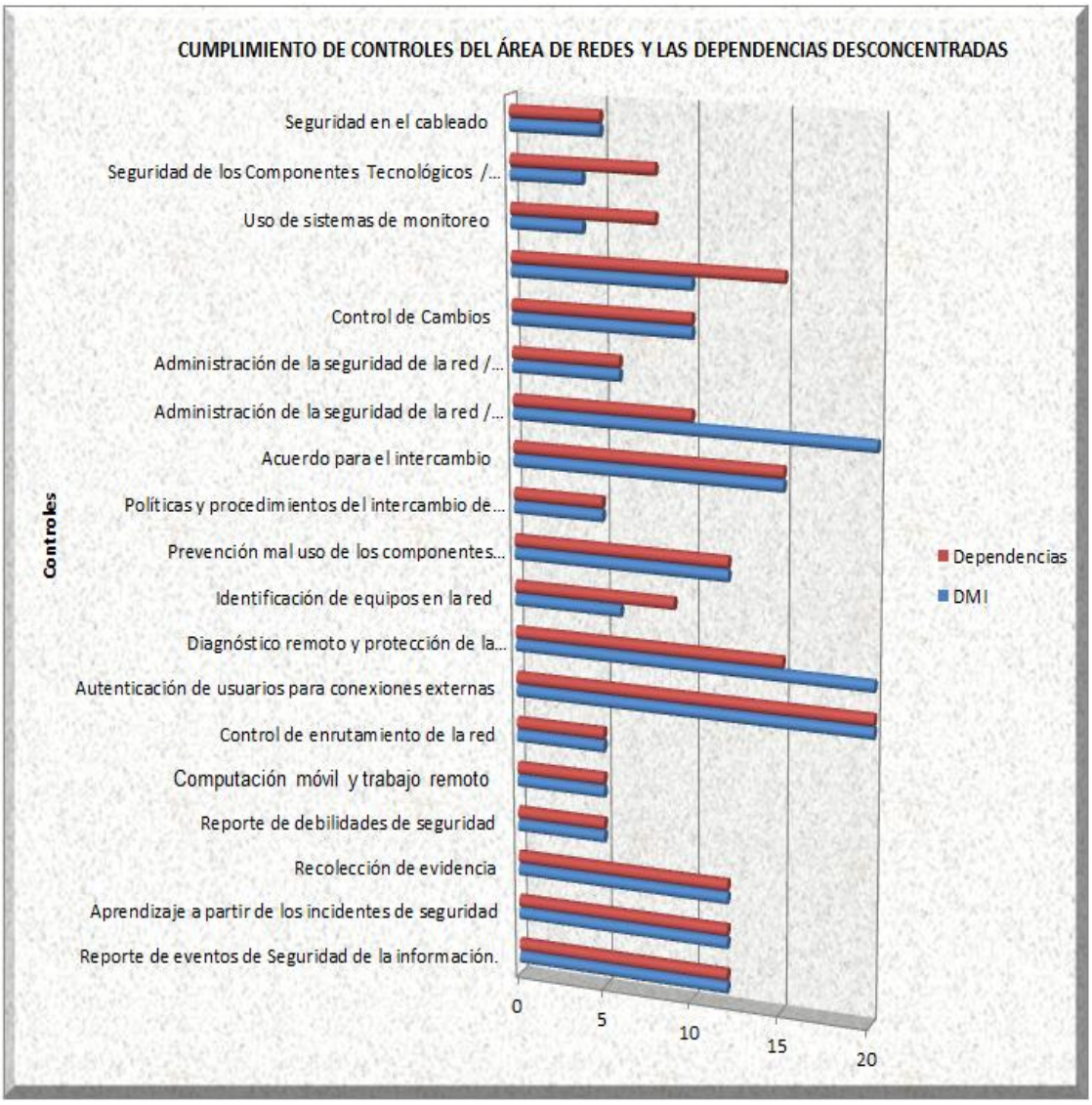

Figura 33. Comparación entre el área de Redes y dependencias desconcentradas, ANEXO 6.2

3.14.1 Cumplimiento de controles de Ingeniería de Soluciones

En la Figura 34, se puede apreciar el cumplimiento de los controles entre la DMI vs las dependencias desconcentradas en las cuales se evidenció que el área que mantiene el control sobre las dependencias desconcentradas es el área de Ingeniería

de Soluciones de la DMI a través de la cual se realiza la adquisición, creación, mantenimiento de los aplicativos que hace uso las dependencias que conforman Municipio de Quito, referente al cumplimiento de los controles se puede apreciar que mantienen un nivel alto de riesgo ya que no existen pruebas de rendimiento, control sobre el código fuente, el personal de la misma forma actúa de forma intuitiva cuando realiza cambios a los aplicativos.

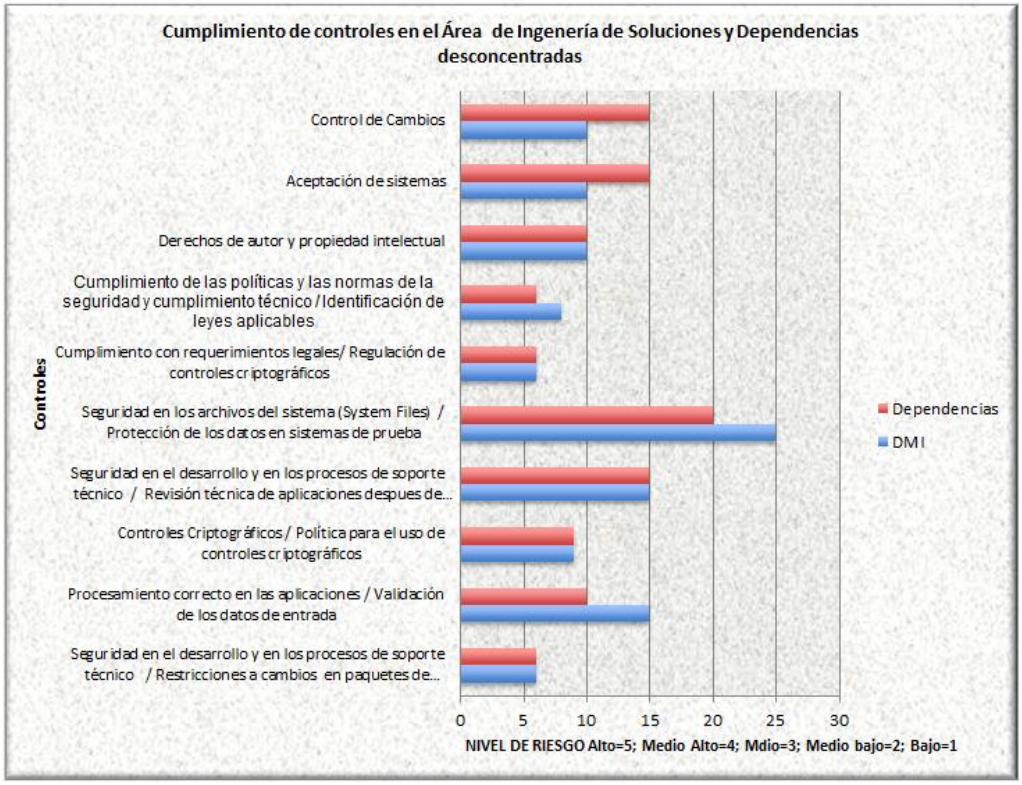

Figura 34. Comparación entre el área de Ingeniería de Soluciones y dependencias desconcentradas, anexo 5,2.

3.14.5 Cumplimiento de controles del área de Producción

El área de Producción es el área más crítica de tecnología ya que se encuentran centralizados servidores, aplicativos, infraestructura, versionamiento, bases de datos, información para lo cual luego del análisis se puede apreciar en el cuadro estadístico que las dependencias desconcentradas se rigen a lo dispuesto por el área de Producción en la mayoría de los casos y en ciertos casos actúan de forma intuitiva ya

que no existen procedimientos que apoyen a mantener un plan de contingencia, un control en los accesos a los diferentes aplicativos, gestores de bases de datos y servidores.

El personal del área tiene conocimientos de seguridad pero no son aplicados puesto que no existen estándares que apoyen a la seguridad de la información, en el cuadro estadístico N 35, se detalla un cuadro comparativo entre la DMI y las dependencias desconcentradas.

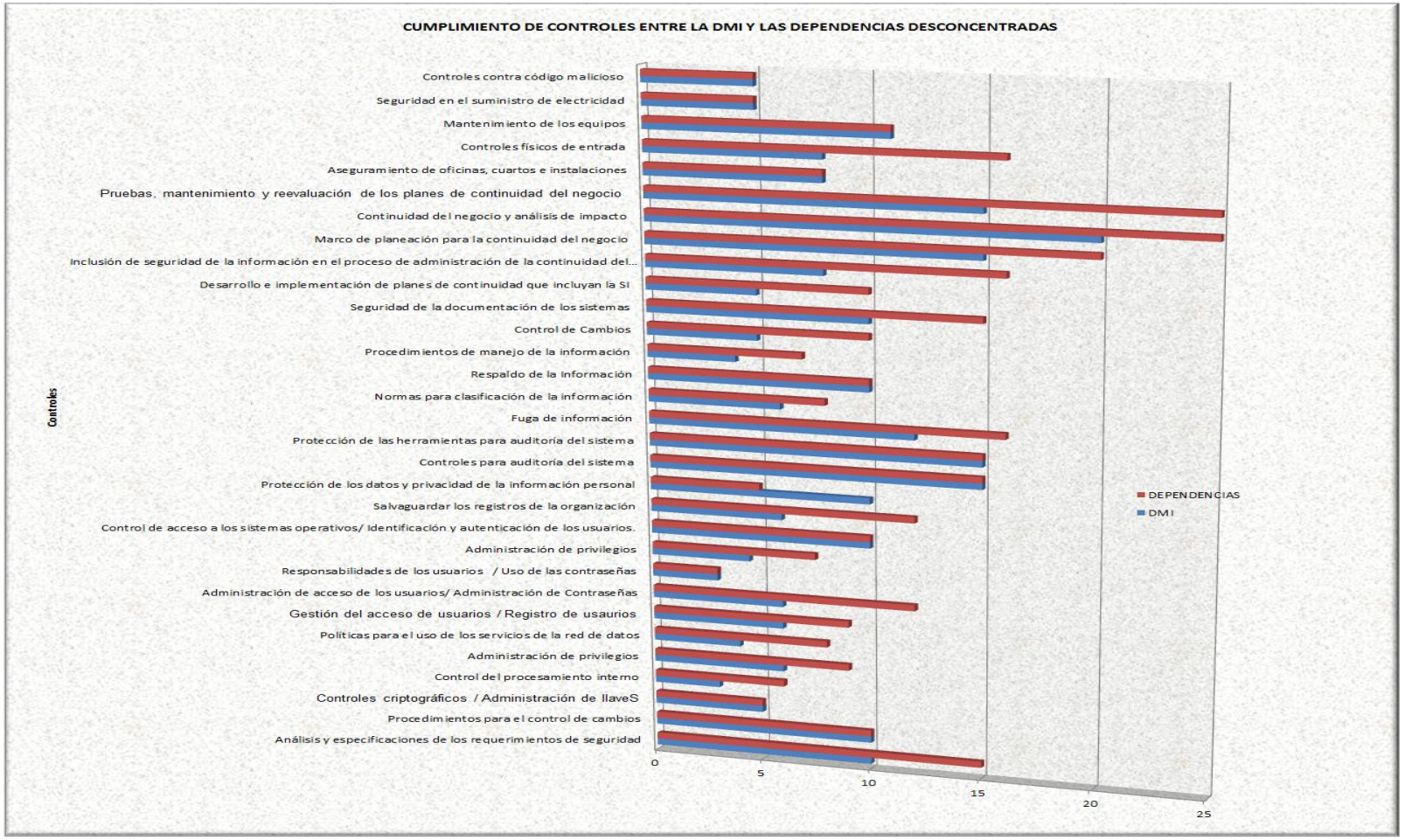

Figura 35. Comparación entre el área de Producción y dependencias desconcentradas, anexo 3.2

En conclusión la mayoría de las áreas presentan “Falla en la operación del servicio”, “Compromiso de la información” la cual es referente a los Errores humanos, Divulgación, Espionaje, manipulación de hardware, manipulación de software, difusión de documentación requirente para la operatividad, entre otros; esto afecta a los recursos de la Institución, siendo vulnerabilidades que son de apoyo para los posibles atacantes externos e internos. En la mayoría de las áreas se puede evidenciar que dejan de a la Seguridad de la Información y esto se debe a las siguientes particularidades:

- Bajo nivel de personal de seguridades de la información.
- Carencia en lineamientos definidos para el ámbito de seguridad.
- Deficiencia en concientización, difusión y capacitación en temas de seguridad de información.
- Deficiencia en la generación de procedimientos que apoyen a las políticas de Seguridad..

Las amenazas primordiales que afectan a las áreas de tecnología son:

- La **pérdida de los servicios esenciales.-** concentra amenazas como pérdida de equipos, pérdida de activos físicos, destrucción de equipos o medios necesarios para que funcione el equipo de la organización. Los servicios y el equipo afectan de manera importante al servicio que representa la imagen de la institución.
- **Compromiso de las funciones.-** se debe a la falta de procedimientos, políticas o documentación que establezca puntualmente actualizaciones, inventario, configuración o adquisición de software, hardware que mantiene o requiere la institución.
- **Falla de la gestión.-** se debe a la falta de difusión referente utilización o restricciones técnicas, o uso tales como:

    - Archivos requisitos relacionados con la organización, gestión de medios

- Arquitectura general relacionada con la existencia de topología o arquitectura física.
- Software de aplicación.- relacionado con el diseño o funcionalidad del software generando problemas en el soporte al usuario de bajo nivel.
- Paquete de software utilización de software desconociendo su funcionalidad.
- Entre otros.

Fallas técnicas.- representan a las amenazas que mantienen a la institución con un nivel alto de dependencia de software ubicándose ahí el incumplimiento del mantenimiento de sistema de información, saturación del sistema de información, entre otros.

3.16 Efectividad de los controles existentes en las áreas de la DMI

Los controles identificados durante el proceso de levantamiento de Información se presentan por tipos de Control y por las áreas de Tecnología de la Dirección Metropolitana de Informática.

Tipo de Control.- contiene la clasificación asignada a las actividades de control.

- No existe control
- Los controles existentes no son efectivos
- Los Controles existentes son efectivos pero no están documentados.
- Los controles son efectivos y están documentados.

Área de Producción

A continuación se detallan los controles de la política de gestión tecnológica que se encuentran en uso, el cual se obtuvo luego de la tabulación realizada a las encuestas del ANEXO 1.3. El resultado se presenta en la Tabla 19.

Tabla 19.

Efectividad de las medidas de control existentes en el área de Producción,

Código de Preguntas	Nivel de exposición de Riesgo actual en la DMI	Control existente de la Política DMI				CRITERIOS PARA EVALUAR LA EFECTIVIDAD DE LAS MEDIDAS DE CONTROL EXISTENTES			
	Estado actual	METODO DE CONTROL DE LA POLÍTICA	No existe	Si cumple	No cumple	NO EXISTEN CONTROL	LOS CONTROLES EXISTENTES NO SON EFECTIVOS	LOS CONTROLES EXISTENTES SON EFECTIVOS PERO NO ESTAN DOCUMENTADOS	LOS CONTROLES SON EFECTIVOS Y ESTAN DOCUMENTADOS
P1	Semanalmente	De la SEGURIDAD DE LOS DATOS.			X		X		
P2	Jefe inmediato	De la SEGURIDAD DE LOS DATOS.		X			X		
P3	Semanalmente	De la SEGURIDAD DE LOS DATOS.		X			X		
P4	Jefe inmediato	De la SEGURIDAD DE LOS DATOS.		X			X		
P5	Los procedimientos de respaldo de base de datos e información está operando y existe evidencia	Inexsistencia	X			X			
P6	Cada vez que existe cambios en la configuraciòn	De la SEGURIDAD DE LOS DATOS.		X			X		
P7	Los procedimientos de almacenamiento de respaldo de información esta operando y existe evidencia	Inexsistencia	X			X			
P8	Claves criptográficas	Inexsistencia	X			X			
P9	Uso de auditorías internas para porbar controles	Inexsistencia	X			X			
P10	Existen procedimientos y existen evidencia documental	Inexsistencia	X				X		

Continúa →

P11	El jefe imediato del áre	De los NIVELES DE CONFIDENCIALIDAD DE LA INFORMACIÓN		X			X		
P12	24 X 7 y está documentado	Inexsistencia	X			X			
P13	Existen procedimientos y existen evidencia documental	Inexsistencia	X			X			
P14	El plan de operaciones esta documentado y aprobado por el DI	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO			X		X		
P15	El plan de operaciones existe poer no está formalizado	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO			X		X		
P16	Bitácora de operaciones y plan de emergencia	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO			X		X		
P17	Acompañamiento del técnico responsable del área	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.		X				X	
P18	El procedimiento está operando y existen evidencia documental	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.			X		X		
P19	Jefe inmediato del área de TI	Mantenimiento de Software			X		X		
P20	Autorización del dueño del proceso	De la Calidad del proceso de una Solución Tecnológica.			X		X		
P21	Ambiente de desarrollo	Inexsistencia	X			X			
P22	Jefe inmediato del área	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.		X				X	
P23	El procedimiento está operando y existen evidencia documental	Inexsistencia	X				X		
P24	Una vez por semana y está documentado	Inexsistencia	X				X		
P25	El procedimiento está operando y existe evidencia documental de su eficiencia y eficacia	Inexsistencia	X				X		
P26	Jefe del área de producción	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.			X			X	
P27	Existencia de un script maestro	De la SEGURIDAD DE LOS DATOS.			X			X	
P28	Alerta del SO sobre actualizaciones	gestion de los recursos informaticos		X					X

Continúa →

P29	El procedimiento está operando y existen evidencia documental	n/a procedimientos		X					X
P30	Clave en texto claro	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.			X		X		
P31	Clave encriptada	De la SEGURIDAD DE LOS DATOS.		X				X	
P32	Licencia perpetua y versión actualizada	GESTION DE LOS RECURSOS INFORMATICOS		X					X
P33	Siempre	Inexsistencia	X			X			
P34	Alerta del SO sobre actualizaciones	Gestión de recursos informaticos CAT			X				
P35	Necesidad de la institución	Gestión de recursos informaticos INFRAESTRUCTURA			X				
P36		De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO		x					
P37		De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO; Seguridad Perimetral							
P38		Inexsistencia	x						
P39		Inexsistencia	X			X			
P40		Inexsistencia	X			X			

Fuente: López & Lala, 2013, anexo 4.1

De acuerdo a las actividades de control obtenidas del resultado de la tabulación de las encuestas verificando el cumplimiento de lo dispuesto en la Política de Tecnología de la DMI se ha obtenido como resultado la presenta estadísticas del análisis de resultados obtenidos por nivel de Cumplimiento, Figura 36

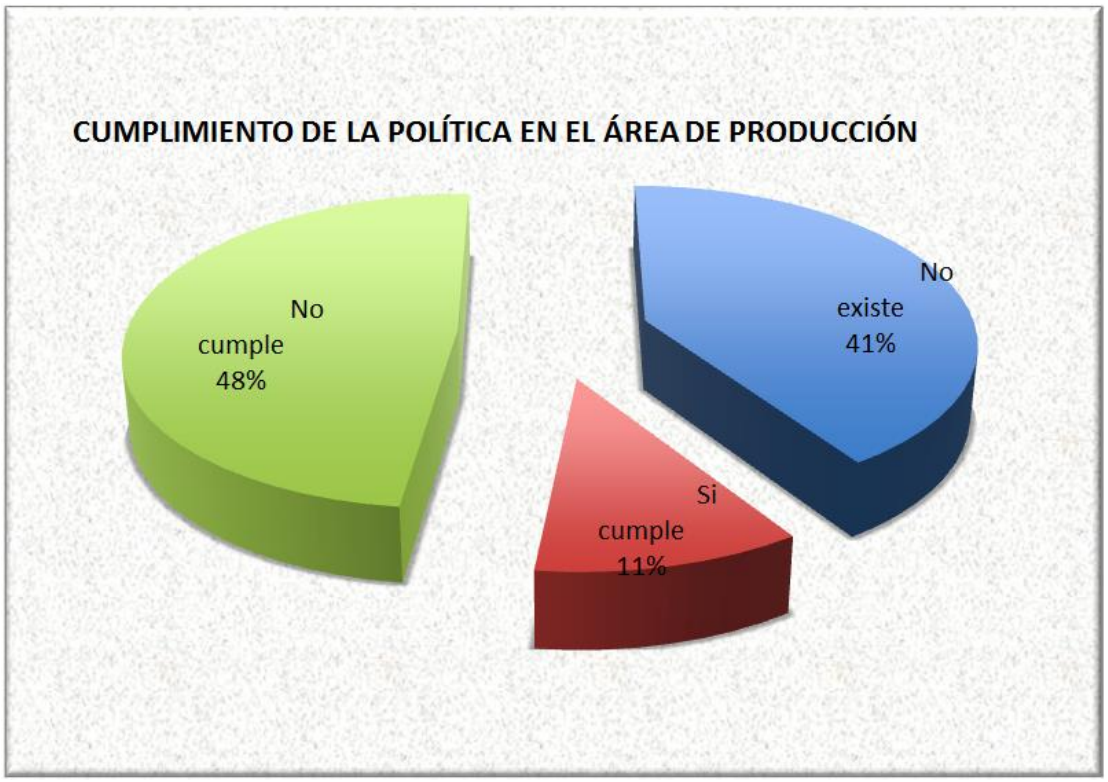

Figura 36. Nivel de Cumplimiento de las políticas de Tecnología de la DMI en el área de Producción

La efectividad que actualmente tienen los controles de la política de gestión tecnológica se muestra en la Figura 37, en lo que se manifiesta lo siguiente:

- El 48% de los controles existentes no son efectivos,
- El 29% no existen controles de cumplimiento afectando el riesgo institucional.

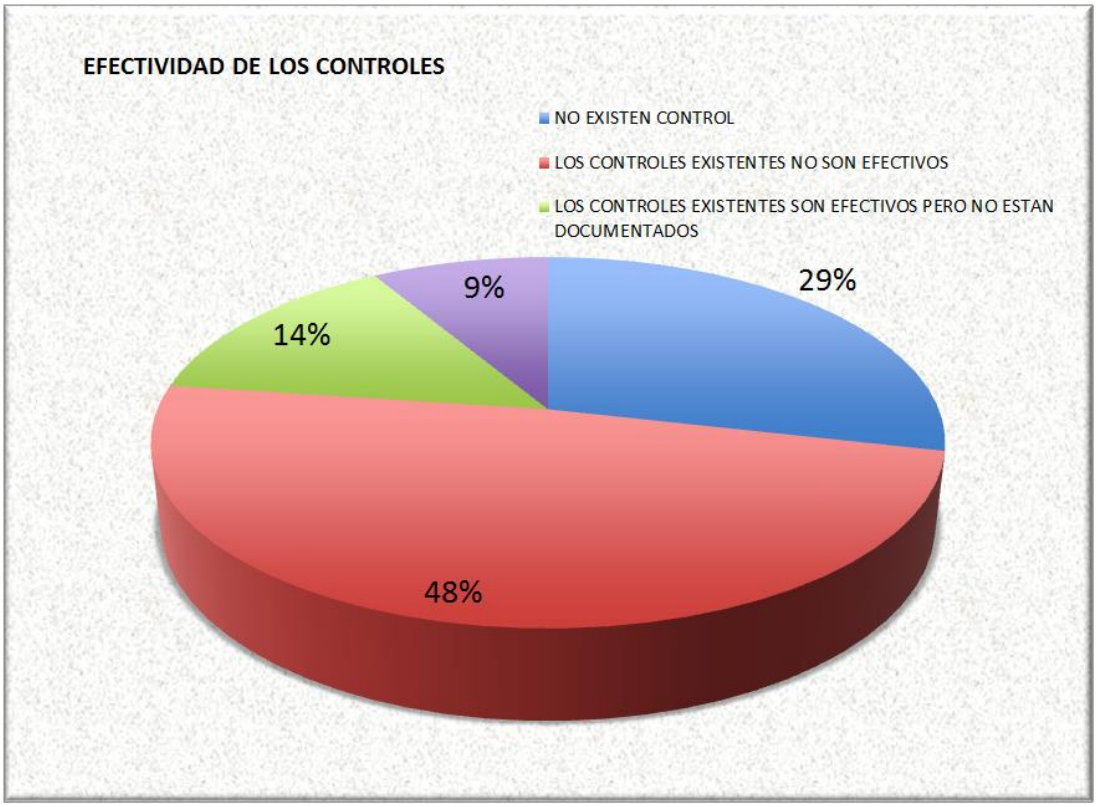

Figura 37. Efectividad de los Controles existentes en el área del Producción, anexo 4.1

Área del CAT(Centro de Atención Tecnológica)

A continuación se detallan los controles de la política de gestión tecnológica que se encuentran en uso en el área del Centro de Atención Tecnológico, el cual luego de la tabulación realizada a las encuestas del ANEXO 1.1.

El resultado se presenta en la Tabla 20 y se evidencia en los resultados que en algunas respuesta no existe un control que se encuentra en la Política de Gestión Tecnológica de la DMI.

Tabla 20.

Efectividad de las medidas de control existentes en el área de Centro de Atención Tecnológico

PREGUNTAS	Nivel de exposición de Riesgo actual en la DMI	Control existente de la Política DMI				CRITERIOS PARA EVALUAR LA EFECTIVIDAD DE LAS MEDIDAS MEDIDAS DE CONTROL EXISTENTES			
	Estado actual	METODO DE CONTROL	No existe	Si cumple	No cumple	NO EXISTEN CONTROL	LOS CONTROLES EXISTENTES NO SON EFECTIVOS	EXISTENTES SON EFECTIVOS PERO NO ESTAN DOCUMENTADOS	SON EFECTIVOS Y ESTAN DOCUMENTADOS
C1	Una vez cada tres meses	Inexsistencia	X			X			
C2	Dueño del proceso	Inexsistencia	X			X			
C3	Niveles de Soporte estan operando y existe evidencia	Inexsistencia	X			X			
C4	Alerta del SO sobre actualizaciones	Inexsistencia	X			X			
C5	El procedimiento de actualización del Software está documento y formalizado	Inexsistencia	X			X			
C6	Necesidad de la institución	Inexsistencia	X			X			
C7	El procedimiento de actualización está operando, es eficaz y eficiente	Parágrafo 3º. : De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO. Art. 8			X		X		
C8	Jefe inmediato	Parágrafo 3º. : Activación y suspensión de cuentas de acceso a Internet Corporativo, Art. 2		X				X	

Continúa →

C9	El procedimiento esta operando y existe evidencia	Uso de Internet, Parágrafo 3º. : Activación y suspensión de cuentas de acceso a Internet Corporativo		X			X		
C10	Jefe inmediato	TITULO II. Del Correo Electrónico, Parágrafo 6º. : Creación y eliminación de cuentas de correo		X				X	
C11	Existe evidencia documental de su cumplimiento	TITULO II. Del Correo Electrónico		X					X
C12	Existe evidencia en el cta detallada del tècnico informático	Parágrafo 3º. : MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS, Art. 2.- MANTENIMIENTO			X		X		
C13	Anualmente	Parágrafo 3º. : MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS			X		X		
C14	Anualmente	Parágrafo 3º. : MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS			X		X		
C15	Está documentado y autorizado por la DMI	Parágrafo 3º. : MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS			X		X		
C16	El repositorio está documentado y autorizado	Parágrafo 5º. : Otros aspectos de la Calidad de Soluciones Tecnológicas, Art. 16.- La factoría de experiencias perseguirá los siguientes beneficios		X				X	
C17	Cada vez que hay cambios	Parágrafo 4º. : De la SEGURIDAD DE LOS DATOS, lit c		X				X	
C18	La difusión se realiza usualmente	Se encuentra en el Capiyulo II, parafo 4º arti. 1 literal c, antener la biblioteca con la documentación de los sistemas de información, productos de aplicación, libros, manuales	X					X	
C19	Cuando existen fallos.	Parágrafo 3º. : De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO, Art. 8, Seguridad Componentes Activos de Cableado.		X			X		

Continúa →

C20	Autorización del funcionario.	Parágrafo 3º. : MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS, Art. 3.- CONTROL			**X**		**X**		
C21	En el rango de Rara vez o nunca.	Parágrafo 3o. : De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO; Seguridad perimetral			**X**			**X**	
C22	Constante y existe evidencia	Parágrafo 3º. : De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO, Art.8, Seguridad Perimetral	**X**				**X**		
c23		Parágrafo 3º. : MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS, Art. 2.- MANTENIMIENTO	**X**					**X**	

Fuente: López & Lala, 2013, anexo 3.1

La presenta estadísticas representa al análisis de resultados obtenidos por nivel de Cumplimiento en el área del Centro de Atención Tecnológica, Figura 38, y la información está consolidada en el anexo 4.

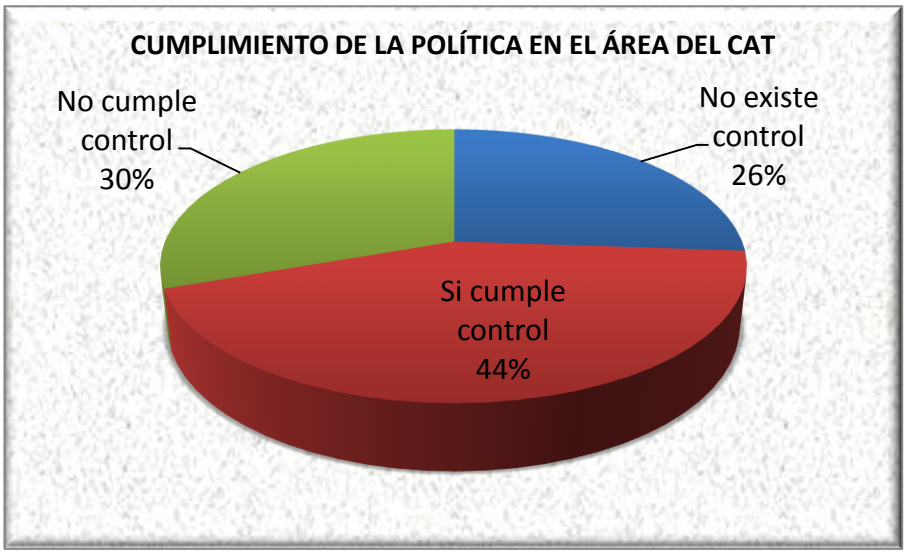

Figura 38. Nivel de Cumplimiento de las políticas de Tecnología de la DMI en el área del CAT, anexo 3.1.

La efectividad que actualmente tienen los controles de la política de gestión tecnológica se muestra en la Figura 39.

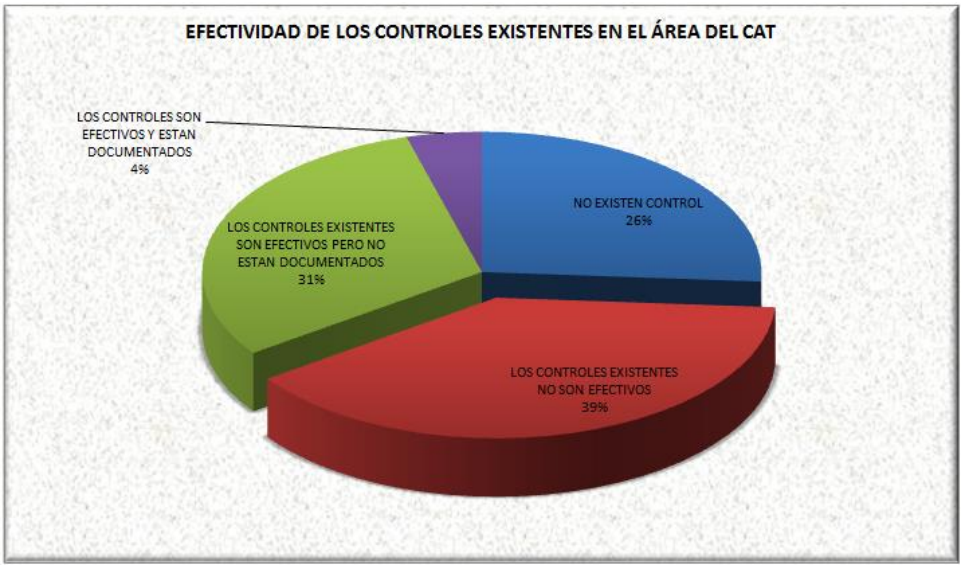

Figura 39. Efectividad de los Controles existentes en el área del CAT, anexo3.1.

Área del Redes

A continuación se detallan los controles de la política de gestión tecnológica que se encuentran en uso en el área del Redes, y se verifican la afectividad de los controles, Tabla 21.

Tabla 21.

Efectividad de las medidas de control existentes en el área de Producción, anexo 3.1

PREGUNTAS	Nivel de exposición de Riesgo actual en la DMI	Control existente de la Política DMI				CRITERIOS PARA EVALUAR LA EFECTIVIDAD DE LAS MEDIDAS DE CONTROL EXISTENTES			
	Estado actual	MÉTODO DE CONTROL	No existe	Si cumple	No cumple	NO EXISTEN CONTROL	LOS CONTROLES EXISTENTES NO SON EFECTIVOS	EXISTENTES SON EFECTIVOS PERO NO	LOS CONTROLES SON EFECTIVOS Y ESTAN DOCUMENTADOS
R1	Director de Informática	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.		x				x	
R2	Por petición	Inexsistencia	x			x			
R3	Alertas en HW	Inexsistencia	x			x			
R4	Acceso por credenciales(usuario y clave)	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.		x				x	
R5	Claves encriptadas	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.		x				x	
R6	Rara vez	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.			x		x		
R7	Rara vez	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.			x		x		
R8	El procedimiento existe pero no esta documentado	Inexsistencia	x			x			
R9	Mensualmente	Inexsistencia	x			x			
R10	Usualmente	Inexsistencia	x			x			
R11	Usualmente	Inexsistencia	x			x			
R12	Mensualmente	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO			x		x		

Continúa →

R13	Cada vez que existe cambios en la configuración	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO		x				x	
R14		Inexsistencia	x					x	
R15		Inexsistencia	x					x	
R16		Inexsistencia	x					x	
R17		Inexsistencia	x						x
R18		Inexsistencia	x						x
R19		Inexsistencia	x						x
R20		Inexsistencia	x					x	

Fuente: López & Lala, 2013, anexo 3.1

La presenta estadísticas representa al análisis de resultados obtenidos por nivel de Cumplimiento en el área del Redes, Figura 38, y la información está consolidada en el anexo 6.

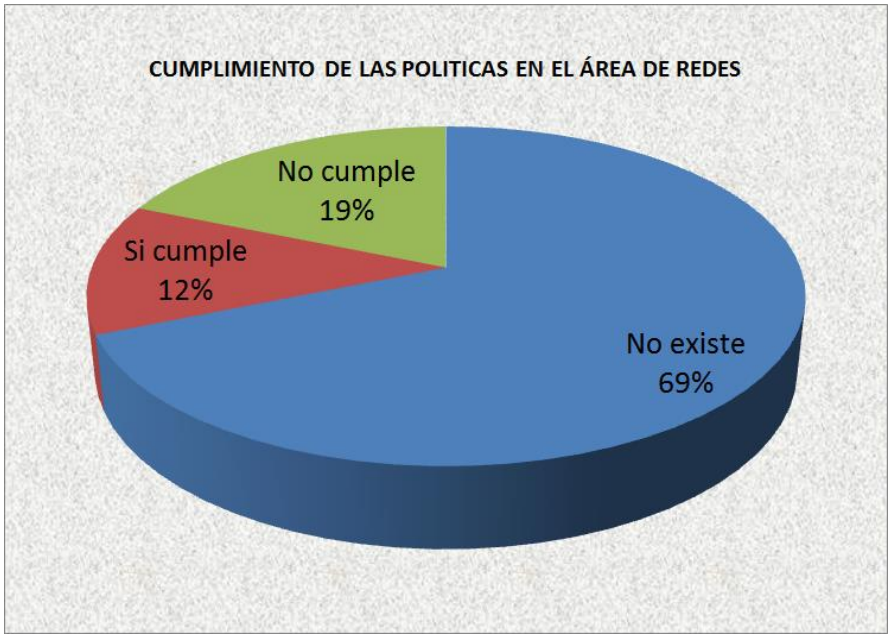

Figura 40. Nivel de Cumplimiento de las políticas de Tecnología de la DMI en el área del Redes anexo 3.1.

La efectividad que actualmente tienen los controles de la política de gestión tecnológica en el área de Redes, se muestra en la Figura 41.

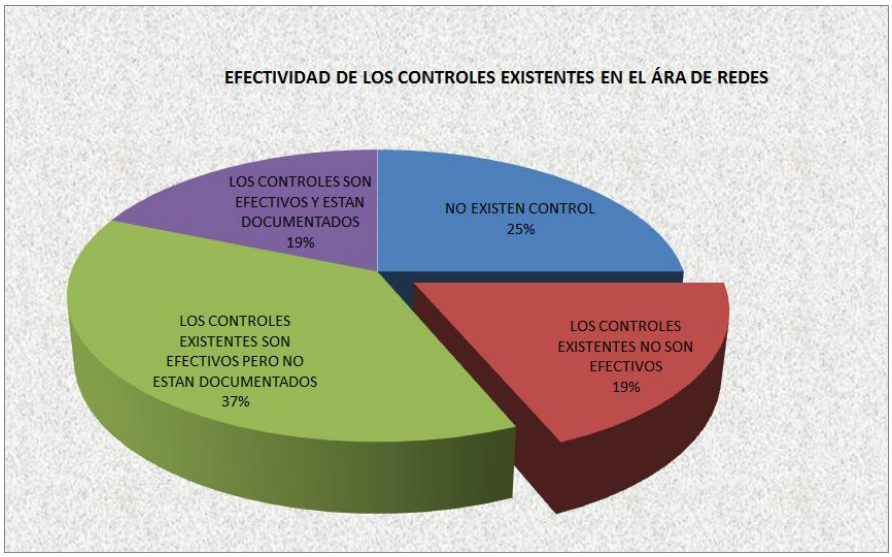

Figura 41. Efectividad de los Controles existentes en el área del Redes, anexo 6.

Área de Ingeniería de Soluciones

A continuación las actividades de control se agrupan por tipo de Control obtenidas en el área de Ingeniería de Soluciones, Tabla 22

Tabla 22.

Control existente agrupado por Tipo de Control de Ingeniería de Soluciones

PREGUNTAS	Nivel de exposición de Riesgo actual en la DMI	Control existente de la Política DMI				CRITERIOS PARA EVALUAR LA EFECTIVIDAD DE LAS MEDIDAS DE CONTROL EXISTENTES			
	Estado actual	METODO DE CONTROL	No existe	Si cumple	No cumple	NO EXISTEN CONTROL	EXISTENTES NO SON EFECTIVOS	EXISTENTES SON EFECTIVOS PERO NO ESTAN	LOS CONTROLES SON EFECTIVOS Y ESTAN DOCUMENTADOS
IS1	Gerente de proyecto	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO			X		X		
IS2	El procedimiento es utilizado y existe evidencia documental	Inexsistencia	X			X			
IS4	No existe procedimientos	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO Art.6			X			X	

Continúa →

IS3	El procedimiento contempla la arquitectura de software está documentada y aprobada por el DI	De la AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO Art.6			X			X	
IS5	Clave en texto claro	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO Art.5		X					X
IS6	Usualmente	Inexsistencia	X			X			
IS7	El procedimiento existe pero no está documentado	De los NIVELES DE SEGURIDAD LÓGICO Y FÍSICO Art.5		X				X	
IS8	No existe procedimientos	Inexsistencia	X			x			
IS9	El programador	Inexsistencia	X			x			
IS10		Art3. de la Contratación		X					x

Fuente: López & Lala, 2013, anexo 5.1

La presenta estadísticas representa al análisis de resultados obtenidos por nivel de Cumplimiento en el área de Ingeniería de Soluciones, Figura 42.

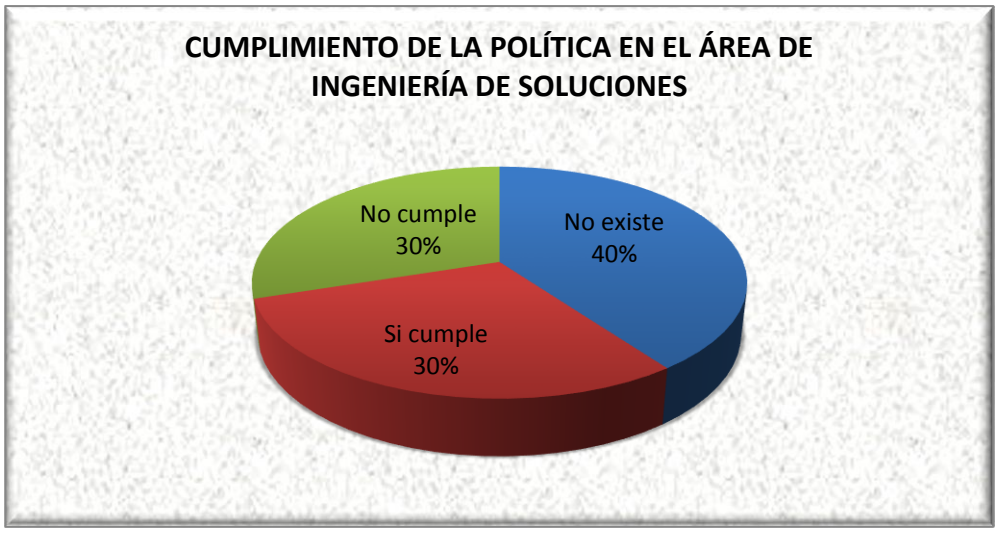

Figura 42, Nivel de Cumplimiento de las políticas Tecnología de DMI en el área del Ing. Soluciones,anexo 5.1

La efectividad que actualmente tienen los controles de la política de gestión tecnológica en el área de Ingeniería de Soluciones, se muestra en la Figura 43.

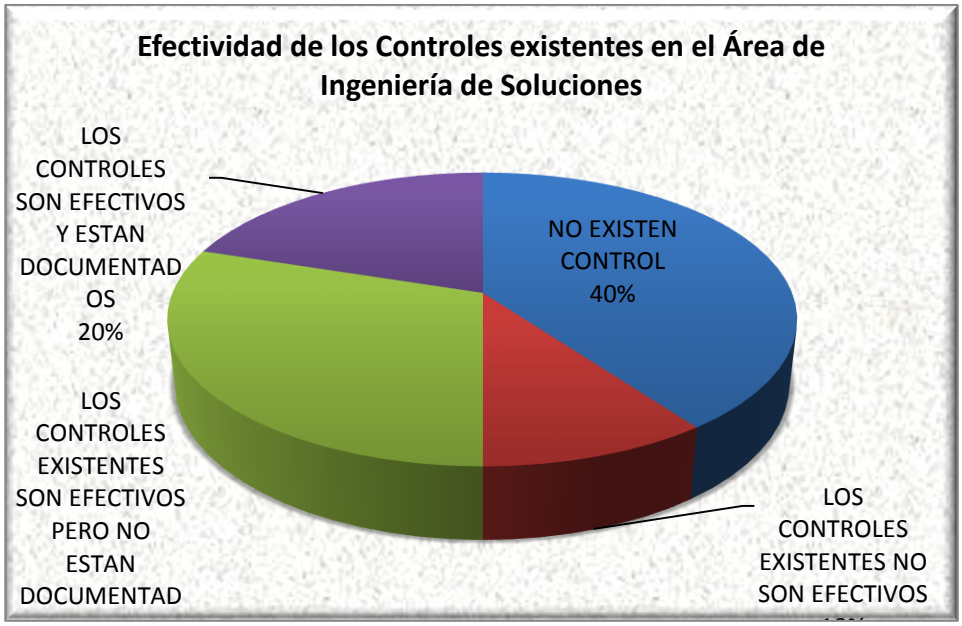

Figura 43. Efectividad de los Controles existentes en el área de Ingeniería de Soluciones, anexo 5.1

3.16.1 Controles existentes en la DMI

Los resultados obtenidos a los controles existentes en las áreas de la Dirección Metropolitana de Informática se agrupan de forma estadística en la Figura 44.

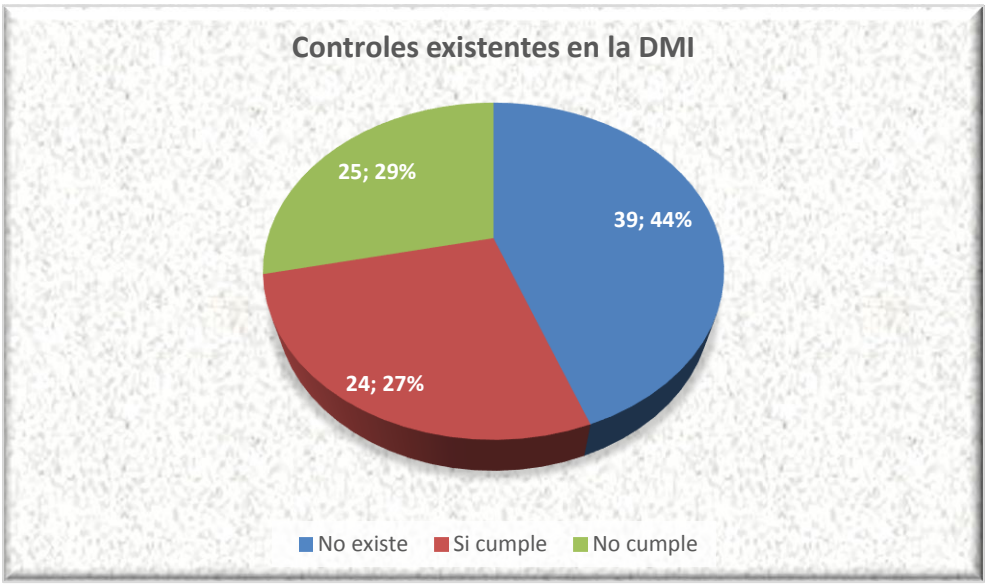

Figura 44. Cumplimiento de controles de la política de gestión tecnológica de la DMI, (López & Lala, 2013).

De acuerdo a los resultados obtenidos el personal de tecnología cumplen la política de la siguiente forma:

- Existe un 39,44% de controles que no se encuentran planteados en la política de gestión tecnológica y se realiza bajo procedimientos generados por el área requirente.
- El 24,27% se cumple con los controles dispuestos en la política de tecnología tanto por la DMI y Dependencias Municipales.
- El 25,29% de los controles existentes no se cumplen.

3.17 Nivel de Madurez De La DMI

¿Cuál es el estado actual del Municipio del Distrito Metropolitano de Quito, a nivel de madurez de aplicación de las mejores prácticas de aseguramiento y monitoreo*?*

Actualmente la Dirección Metropolitana de Informática presenta una política de gestión tecnológica la misma que no certifica los temas de seguridad de la Información.

De acuerdo a los datos obtenidos por parte de los funcionarios entrevistados de las dependencias desconcentradas y DMI el compromiso se encuentra en validar el cumplimiento de los controles de la política de gestión tecnológica, el cual se realizó bajo un análisis de seguridad.

El área de base de datos, QA, producción, redes, Ingeniería de Soluciones cuenta con Administradores, Coordinadores o jefes de equipo encargados de actividades administrativas y operativas que ajustan con prácticas básicas a nivel de seguridad de la información como uso de contraseñas y contraseñas seguras.

El área del CAT (Centro de Atención Tecnológico) de acuerdo a los procesos del área cumple con labores de soporte en sitio a solicitudes de pre configuración de equipos, instalación, soporte a sistemas operativos y aplicaciones de software cumpliendo también con la creación de perfiles básicos de usuario.

Es importante acotar que concluidas las entrevistas se pudo identificar que las áreas de las dependencias cubren distintos aspectos de seguridad de la información de forma independiente; cabe indicar que la organización no cuenta con el área de seguridad por lo que necesita adoptar prácticas que permitan gestionar la seguridad de la información.

Al realizar la validación frente a los objetivos de control de la norma ISO 27002 con apoyo de la métrica CMM de COBIT se estableció que los niveles de madurez alcanzados son de grado 0 "No existente" en algunos dominios y el máximo nivel de madurez encontrado es de "3" procesos definidos.

3.17.1 Presentación de Resultados

A continuación se emiten los criterios del análisis de la ISO27002 por cada dominio.

Política de seguridad de la información:La existencia, revisión y cumplimiento de políticas de Seguridad de la Información son apoyadas en el documento de políticas de gestión tecnológica la misma que está enfocada a brindar directrices generales en todos los aspectos de tecnología pero no se enfoca a la seguridad de la información, para lo cual se requiere definir, documentar las directrices con un alcance definido a la seguridad, se encuentra en un nivel 1"existencia", se requiere trabajar en implementar políticas de Seguridad ver Tabla 23

Tabla 23

Analisis en el dominio de política de seguridad de la información.

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
5,1	Política de Seguridad de la Información			5,0%
5.1.1	NO	**0**	Documentar e implementar la política de seguridad de la información.	0,05
5.1.2	NO	**0**	Al complementar el documento de política, se deberá dejar explícita la tarea periódica de revisión y evaluación en unas fechas formales.	0,05

Fuente: López & Lala, 2013, anexo 8

Organización de la seguridad de la información.- Existe el compromiso y la voluntad por parte de las directivas a nivel del área de Tecnología; pero no se implementa controles de este dominio por lo que se encuentran en un nivel 1"existencia", se requiere trabajar en controles básicos tales como depuración de roles y perfiles con asignación forma de responsabilidades, ver Tabla 24.

Tabla 24

Análisis en el domunio de Organización de la seguridad de la información

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
6,1	Organización Interna			5%
6.1.1	NO	**1**	Un programa de conciencia en seguridad de la información que reuna a los directivos de la institución	0,1
6.1.2	NO	**1**	Crear el área de Seguridad para fortalecer esquemas de capacitación en seguridad	0,1
6.1.3	NO	**1**	Crear el área de Seguridad para fortalecer esquemas de capacitación en seguridad	0,1
6.1.4	NO	**1**	Reforzar los esquemas de mantenimiento de documentos de auditorías de seguridad, como administración de Logs, revisión de bitácoras y monitoreo de incidentes en áreas de procesamiento de datos	0,1
6.1.5	NO	**1**	Este punto tiene una especial madurez, incluyendo esquemas de estudios de seguridad y sanciones claramente especificadas	0,1
6.1.6	N/A	**1**	N/A	0,1
6.1.7	NO	**1**	Crear el área de Seguridad para fortalecer esquemas de capacitación en segurdad	0,1
6.1.8	NO	**1**	Realizar un cronograma anual para realizar auditorías de control interno en el área de Tecnología	0,1
6,2	Terceros			5%
6.2.1	NO	**1**	Alinear con la implementación del SGSI, los análisis de riesgo externos e internos sobre los activos e información.	0,1
6.2.2	NO	**1**	Certificar la entidad en ISO 27001 o mostrar el cumplimiento sobre la norma, reiteraría y daría amplia fuerza al concepto de seguridad de la información que tienen los clientes.	0,1

Continúa →

6.2.3	NO	**1**	Incluír la política de seguridad en los acuerdos y contratos con terceros.	0,1

Fuente: López & Lala, 2013, anexo 8

Gestión de activos.- Este dominio se encuentra en nivel de madurez 1 (inicial), dada la relevancia de la información física y lógica se mantienen controles automatizados adecuados para el uso correcto de tecnologías tales como correo electrónico y acceso a internet; pero es primordial desarrollar un apropiado conjunto de procedimientos para clasificar y manejar la información, ver tabla 25.

Tabla 25

Análisis en el dominio de Gestión de activos

ISO Ref	**Aplica (SI/NO)**	**Cumplimiento**	**Oportunidad de mejora**	**%**
7,1				38 %
7.1.1	Si	**3**	Centralizar el inventario de todos los activos en un sistema centralizado, enmarcado en un procedimiento y asignado a un responsable de la dependencia centralizada por su mantenimiento.	0,75
7.1.2	Si	**3**	Los responsabilidades sobre los activos de información se encuentra ligada a la información del empleado.	0,75
7.1.3	Si	**3**	Incluír el uso aceptable de los activos tecnológicos en el manual de funciones de los empleados	0,75
7,2				13 %
7.2.1	Si	**1**	Se intuye la clasificación de la información.	0,25
7.2.2	Si	**1**	El esquema de manejo de la información debe estar apoyado cuando se cree la política de Seguridad de la Información.	0,25

Fuente: López & Lala, 2013, anexo 8

Seguridad de los recursos humanos.- Este dominio se encuentra en nivel de madurez 1 (inicial), dado que no existe un procedimiento establecido para tratar el tema de seguridad en el recurso humano, para lo cual es primordial desarrollar un

apropiado conjunto de procedimientos para la contratación del recurso humano, ver tabla 26.

Tabla 26

Análisis en el dominio de Seguridad de recursos humanos

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
8.1	Previo a la contratación			12%
8.1.1	Si	**0**	Contar con los perfiles mínimos para cumplir los roles faltantes necesarios. Incluír las responsabilidades de seguridad	0.5
8.1.2	Si	**5**	Mantener el control implementado y describir el procedimiento dentro del SGSI	0.1
8.1.3	Si	**5**	Mantener el control implementado y describir el procedimiento dentro del SGSI	0.1
8.2	Durante el empleo			12%
8.2.1	Si	**3**	La participación en seguridad de las directivas se realiza más que por su intención en el fortalecimiento de la seguridad, por requerimiento y regulaciones. Esto puede mejorar con un plan de conciencia a nivel directivo	0.5
8.2.2	Si	**2**	Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI	0.1
8.2.3	Si	**3**	Incluir el detalle de procesos disciplinarios y descargos, dentro del manual de funciones, y en el SGSI	0.1
8.3	Terminación del contrato o cambio de empleo			12%
8.3.1	Si	**3**	Incluir el proceso en el SGSI cuando haya sido implementado	0.5
8.3.2	Si	**3**	Incluir el proceso en el SGSI cuando haya sido implementado	0.1
8.3.3	Si	**2**	Si bien se realizan las actividades de control sobre los privilegios ya no necesarios, no es una actividad formalizada. Debe establecerse un procedimiento formal y consistente dentro del SGSI	0.1

Fuente: López & Lala, 2013, anexo 8

Seguridad física y del entorno.- Este dominio se encuentra en un nivel de madurez en un intervalo entre 1 y 3; las áreas dentro de las instalaciones mantienen

un control pero es necesario fortalecer los controles en la seguridad de los equipos, ver tabla 27.

Tabla 27

Análisis del dominio de Seguridad física y ambiental

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
9,1	Areas Restringidas			25%
9.1.1	Si	**3**	Realiza la revisión periódica del funcionamiento de estos procedimientos y controles	0,5
9.1.2	Si	**3**	Mantener el esquema.	0,5
9.1.3	Si	**3**	Incluír la descripción de las precauciones de seguridad en oficinas	0,5
9.1.4	Si	**3**	Las oficinas mantienen un control a los equipos de seguridad.	0,5
9.1.5	Si	**3**	No descuidar los controles de acompañamiento y registro de todos los usuarios que ingresan a áreas restringidas	0,5
9.1.6	Si	**3**	Incluír poíticas de acceso por áreas de carga y descarga en la Política de Seguridad	0,5
9,2	Seguridad de los Equipos			29%
9.2.1	Si	**2**	Debe implementarse un esquema explicita o una política dentro de la politica que requiera la protección y ubicación de los equipos tecnológicos en areas protegidas	0,75
9.2.2	Si	**3**	Se debe mantener el esquema de UPSs y plantas eléctricas en óptimas condiciones	0,75
9.2.3	Si	**3**	Mantener el esquema. Se debe también eliminar todo cableado obsoleto o en desuso lo antes posible.	0,5
9.2.4	Si	**3**	Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos.	0,75
9.2.5	Si	3	El SGSI debe dictaminar las políticas de uso de equipos de cómputo fuera de las instalaciones de la organización que permitan a directivos, conocer los requerimientos de seguridad para el uso de estos elementos	0,1

Fuente: López & Lala, 2013, anexo 8

Gestión de operaciones y comunicaciones.- Este Dominio se encuentra en un nivel de madurez que se encuentra en un intervalo de 0 a 3 el cual indica que cumple en algunos controles pero no en todos, concentra la mayoría de controles en soluciones

de nivel técnico, operativo olvidando procedimientos establecidos por la institución, ver tabla 28.

Tabla 28

Análisis del dominio de Gestión de operaciones y comunicaciones

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
10,1				5%
10.1.1	Si	**2**	Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia.	0,5
10.1.2	Si	**2**	Los registros de control de cambios deben incluír los elementos de seguridad necesarios, la protección y revisión de los mismos	0,5
10.1.3	Si	**2**	No existe el área de seguridad de la información	0,5
10.1.4	Si	**2**	Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. Debe existir incluír lineamientos de manejo de los datos en Desarrollo y Pruebas.	0,5
10,2				0
10.2.1	Si	**0**	Implementar política de seguridad que permita mantener el registro y políticas de seguridad sobre terceros.	
10.2.2	Si	**0**	Implementar política de seguridad que permita mantener el registro y políticas de seguridad sobre terceros.	
10.2.3	Si	**0**	Implementar política de seguridad que permita mantener el registro y políticas de seguridad sobre terceros.	
10,3				5%
10.3.1	Si	**2**	Se realizan los controles de monitoreo sobre capacidad de recursos, sin embargo la migración a los nuevos recursos toma mas tiempo del esperado.	
10.3.2	Si	**2**	Algunos sistemas ya aceptados para migración, se han demorado en su puesta en producción (Nueva nómina, Sistemas operativos, Bases de datos)	0,5
10,4				2%
10.4.1	Si	**3**	Mantener el esquema de revisión a toda la red, incrementar los controles manualmente a equipos detectados con infección. Realizar una revisión completa cada cierto periodo de tiempo, se recomienda cada mes para activos críticos.	0,25

Continúa →

10.4.2	Si	**0**	El control mas adecuado para la primera línea de defensa en contra de este tipo de malware es la segmentación de la red. Control que no se encuentra adecuadamente implementado.	0,1
10,5				5,0%
10.5.1	Si	**3**	Mantener el esquema de backups y extenderlo a sistemas de información alterantivos como son los usuarios finales.	0,5
10,6				3%
10.6.1	Si	**1**	Se debe replantear la arquitectura de seguridad en la red LAN, para ubicar y configurar correctamente todos los elementos de seguridad y monitoreo en la red. Esto debe esta acompañado de una política de seguridad en el SGSI	0,25
10.6.2	Si	**1**	Segmentar de forma lógica la red, para mantener un adecuado control sobre todos los servicios de red.	0,25
10,7				4%
10.7.1	Si	**1**	Documentar y mantener el control e incluír la política y sus excepciones.	0,1
10.7.2	Si	**2**	Es necesario establecer una política rigurosa acompañada de un procedimiento para la destrucción de medios específicamente identificados.	0,1
10.7.3	Si	**2**	Los manuales de uso de los sistemas son almacenados por parte de los responsables de los mismos. Sin embargo no hay una formalidad en el almacenamiento de procedimientos e inventario de manuales y otros documentos	0,75
10.7.4	Si	**2**	No hay una formalidad en el almacenamiento de procedimientos e inventario de manuales y otros documentos	0,75
10,8				8%
10.8.1	Si	**2**	Incluír en la política y procedimientos claros del intercambio de información	0,75
10.8.2	Si	**2**	El manejo de información y su intercambio con terceros debería incluír acuerdos sobre su transporte y almacenamiento seguros al tratar y manipular la información (por ejemplo comprimir y cifrar la información)	0,75
10.8.3	Si	**1**	En los casos en que sea necesario transportar información, debe exigirse el cumplimiento de una política de protección para esta información.	0,75
10.8.4	Si	**3**	Se debe mantener el esquema de seguridad sobre el correo a nivel de contingencias, antivirus, antispam y revisar periódicamente la efectividad de todos los controles	0,75
10.8.5	Si	**2**	Los controles sobre las plataformas del proceso son adecuados pero hace falta la documentación y políticas formales implementadas	0,75

Continúa →

10,9				1%
10.9.1	No	-	N/A	0,1
10.9.2	No	-	N/A	0,1
10.9.3	Si	**3**	Implementar procedimientos que aseguren la información pública	0,1
10.10				1%
10.1.0.1	Si	**0**	Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros.	0,1
10.1.0.2	Si	**1**	Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso.	0,1
10.1.0.3	Si	**0**	Formar el área de seguriad para que el acceso a los registros sean exclusivos para los auditores, administradores de la plataforma y oficial de seguridad.	0,1
10.1.0.4	Si	**0**	Definir el procedimieto de monitoreo y su relación con el de reacción a incidentes.	0,1
10.1.0.5	Si	**0**	Realizar las revisiones periódicas, definir el procedimieto de monitoreo y su relación con el de atencion de incidentes.	0,1
10.1.0.6	Si	**1**	Se debe diseñar e implementar un procedimiento de sincronización de todos los Sistemas y Aplicaciones, con un sistema unificado para toda la plataforma tecnológica de la organización.	0,1

Fuente: López & Lala, 2013, anexo 8

Control de acceso.- Este dominio se encuentra en un nivel de madurez que se encuentra en un intervalo de 1 a 3, los ítems más importantes por trabajar son la revisión de los derechos de acceso de los usuarios, limitación de tiempo de conexión, computación móvil, entre otros, ver tabla 29.

Tabla 29

Análisis del dominio de Control de acceso

ISO Ref	**Aplica (SI/NO)**	**Cumplimiento**	**Oportunidad de mejora**	**%**
11,1				No existe
11.1.1	SI	**0**	Diseñar e implementar una política de control de acceso de usuarios que incluya los procesos necesarios para autorización y control de acceso a los SI	
11,2				No existe

Continúa →

11,2				No existe
11.2.1	SI	**1**	Diseñar e implementar una política de control de acceso de usuarios que incluya los procesos necesarios para autorización y control de acceso a los SI, incluír en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
11.2.2	SI	**1**	Mantener el esquema implementado. Sin embargo existen esquemas que deben ser revisados tales como Bases de Datos ya que no existe un control formal	
11.2.3	SI	**1**	Documentar una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.	
11.2.4	SI	**1**	Definir la periodicidad y detalle del procedimiento de revisión de privilegios.	
11,3				No existe
11.3.1	SI	**2**	Realizar el plan de concientización y entrenamiento debidos con respecto al tema	
11.3.2	SI	**0**	Realizar el plan de concientización y entrenamiento debidos con respecto al tema	
11.3.3	SI	**0**	Realizar el plan de concientización y entrenamiento debidos con respecto al tema	
11,4				14%
11.4.1	SI	**1**	Implementar un procedimiento de control de equipos conectados a la red, empleando herramientas tecnológicas o políticas de conexión e inventariado.	1
11.4.2	SI	**1**		1
11.4.3	SI	**1**		1
11.4.4	SI	**1**		1
11.4.5	SI	**1**		1
11.4.6	SI	**1**		1
11.4.7	SI	**1**		1
11,5				14%
11.5.1	SI	**3**	Existe procedimientos que permiten realiza las actividades de inicio de sesión	1
11.5.2	SI	**3**	Existe procedimientos que permiten realiza las actividades de inicio de sesión	1
11.5.3	SI	**3**	Mantener el esquema implementado. Extender el esquema a aplicaciones	1
11.5.4	SI	**1**	Mantener el esquema implementado. Extender las restricciones en el dominio para todos los usuarios finales.	

Continúa →

11.5.5	SI	**1**	Debe implementarse políticas de seguridad que protejan el time out para las estaciones de trabajo.	
11.5.6	SI	**1**	Debe implementarse políticas de seguridad que protejan los periodos de tiempo de conexión en los aplicativos.	
11,6				14%
11.6.1	SI	**3**	Extender los controles a las aplicacionoes que ya no lo permiten por medio de controles adicionales como el Directorio activo o un Firewall de Host.	1
11.6.2	SI	**0**	Los sistemas más críticos como bases de datos y servidores de aplicaciones se encuentran aislados en una granja de servidores, sin embargo es necesario hacer lo mismo con los servidores de desarrollo o pruebas que manejan la misma información.	
11,7				14%
11.7.1	SI	**0**	Diseñar e implementar una política de control de computación móvil, acompañada del procedimiento adecuado de control a ciertos equipos.	1
11.7.2	SI	**0**	Consular a la alta directiva sobre temas de teletrabajo.	

Fuente: López & Lala, 2013, anexo 8

Adquisición, desarrollo y mantenimiento de software: Este dominio se encuentre en nivel de madurez en un intervalo entre 1 o 2, sin embargo se requiere implementar controles criptográficos, seguridad en el desarrollo y en los procesos de soporte técnico, ver tabla 30.

Tabla 30

Análisis del dominio de Desarrollo , mantenimiento y adquisición de sistemas

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
12,1				8%
12.1.1	Si	**2**	Debe implementarse una guía con lineamientos claros, que exija lineamientos en el desarrollo y puesta en marcha de nuevos sistemas de información.	0,5
12,2				8%

Continúa →

12.2.1	Si	**2**	Implementar un estándar de desarrollo seguro de aplicaciones que cumpla con políticas específicas de seguridad	0,5
12.2.2	Si	**2**		0,5
12.2.3	Si	**2**		0,5
12.2.4	Si	**2**		0,5
12,3				5%
12.3.1	Si	**1**	Los esquemas criptográficos deben ser obligatorios para el manejo y transporte de información. Este esquema debe ser formalmente descrito en una política de Seguridad	0,75
12.3.2	Si	**1**	una vez implementados los controles criptográficos, es necesario definir e implementar una política y procedimiento de administración de llaves criptográficas.	0,75
12,4				5%
12.4.1	Si	**2**	Mantener el esquema implementado de revisión de sistemas y de puesta en producción. No se debe permitir en ningún caso la instalación de software sin el permiso adecuado.	0,75
12.4.2	Si	**2**	Implementar esquemas de protección de los datos de producción, cambiandolos o eliminando completamente los mismos al terminar las pruebas. Este escenario cambiaría el esquema actual de usar el servidor de pruebas y desarrollo como contingencia de producción.	0,75
12.4.3	Si	**2**	Mantiene el esquema implementado. El procedimiento está alineado a la política de gestión pero no es utilizada completamente	0,75
12,5				3%
12.5.1	Si	**1**	No existe una política que detalle información de seguridad en el desarrollo .	0,5
12.5.2	Si	**1**	No existe una política que detalle información de seguridad en el desarrollo .	0,5
12.5.3	Si	**1**	Mantener el esquema implementado referente a los procedimientos de control de cambios en los procesos de soporte técnico.	0,5
12.5.4	Si	**1**	No existe control que fortalezca el esquema de protección contra fugas de información empleando todos los controles necesarios (técnicos, políticas, acuerdos, etc.)	4
12.5.5	Si	**1**	Mantener el esquema implementado. Sin embargo se debe crear una guía fundamental de principios de seguridad a tener en cuenta por parte de los terceros.	0,5
12,6				2%
12.6.1	Si	**1**	Debe implementarse un esquema de pruebas internas (ya sea por capacitación de un funcionario o por un sistema) que permita una revisión periódica interna al respecto	0,1

Fuente: López & Lala, 2013, anexo 8

Gestión de incidentes de seguridad.- Este dominio se encuentra en nivel de madurez en un intervalo entre 1 o 2, para lo cual se requiere documentar el detalle de los procedimientos relacionados con recolección de evidencias para evidenciar la continuidad del incidente, ver tabla 31.

Tabla 31

Análisis del dominio de Administración de incidentes de SI

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
13,1				38%
13.1.1	Si	**2**	Identificar los incidentes relacionados con la seguridad de la información y su reporte; para dar seguimiento en la mesa de ayuda	0,75
13.1.2	Si	**2**	Identificar los incidentes relacionados con la seguridad de la información y su reporte; para dar seguimiento en la mesa de ayuda	0,75
13,2				13%
13.2.1	Si	**1**	Documentar y divulgar formalmente el proceso de incidentes de seguridad	0,25
13.2.2	Si	**1**	Realizar la revisión a todos los repotes de incidentes e incluírlos en el plan de mejoramiento; en apoyo con el área de seguridad a implementarse en la institución	0,25
13.2.3	Si	**1**	Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita obtener toda la información necesaria.	0,25

Fuente: López & Lala, 2013, anexo 8

Gestión de la Continuidad del negocio.- Este dominio se encuentra en nivel de madurez 1(inicial), el personal arriesga la estabilidad de la organización ya que no existen procedimientos relacionados para superar eventos catastróficos que afectarían a la operación normal del funcionamiento de la institución, ver tabla 32.

Tabla 32

Análisis del dominio Gestión de continuidad de negocio

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
14,1				32%
14.1.1	Si	**1**	Una vez implementada la política de seguridad, incluírla en el desarrollo de los planes de continuidad del negocio y establecer planes para todos los procesos críticos.	0,5
14.1.2	Si	**1**	Debe existir un análisis periódico de tipo BIA y análisis de riesgos que haga particular detalle en las amenazas inherentes a la organización. Esta actividad se madurará con cada ciclo del SGSI	0,25
14.1.3	Si	**1**	Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.	0,5
14.1.4	Si	**1**	Unificar los términos de análisis para el impacto y los riesgos evaluados en los planes de continuidad del negocio.	0,25
14.1.5	Si	**1**	Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados.	0,1

Fuente: López & Lala, 2013, anexo 8

Cumplimiento.- Este dominio se encuentra en nivel de madurez con intervalo de (1 o 2) por lo que es necesario poner énfasis en el cumplimiento técnico, controles para auditoría del sistema de información, ver tabla 33.

Tabla 33

Análisis del dominio Cumplimiento y normatividad legal

ISO Ref	Aplica (SI/NO)	Cumplimiento	Oportunidad de mejora	%
15,1				3%
15.1.1	Si	**2**	Extender la investigación de legislaciones aplicables a los temas de seguridad de la información.	0,1
15.1.2	Si	**2**	Implementar política de seguridad respecto a derechos de autor	0,1
15.1.3	Si	**2**	Establecer procedimientos especiales de seguridad para los registros organizacionales.	0,1
15.1.4	Si	**2**	Implementar política de seguridad respecto a la protección de datos	0,1
15.1.5	Si	**2**	Establecer controles además de la conciencia institucional, que permitan administrar y monitorear el uso de los componentes tecnológicos.	0,1

Continúa →

15.1.6	Si	**2**	Debe realizarse la adecuada revisión de cuales regulaciones afectan el uso de controles criptográficos y considerarlos para su implementación	0,1
15,2				17%
15.2.1	Si	**2**	Una vez establecida e implementada la política de seguridad, realizar los controles al cumplimiento de la misma	0,5
15.2.2	Si	**2**	Reforzar las revisiones a los planes de mejoramiento y pruebas de vulnerabilidad a los SI.	0,5
15,3				3%
15.3.1	Si	**1**	Documentar e implementar los casos y controles a tener en cuenta para las actividades de auditoría sobre sistemas en producción.	0,1
15.3.2	Si	**1**	Implementar la política de auditoría de sistemas en términos de seguridad de la información y especificar cuáles son las herramientas para la actividad y sus protecciones	0,1

Fuente: López & Lala, 2013, anexo 8

A continuación se comparan los niveles de madurez alcanzados con cada dominio de la norma ISO 27002 frente a las prácticas recomendadas, ver figura 45.

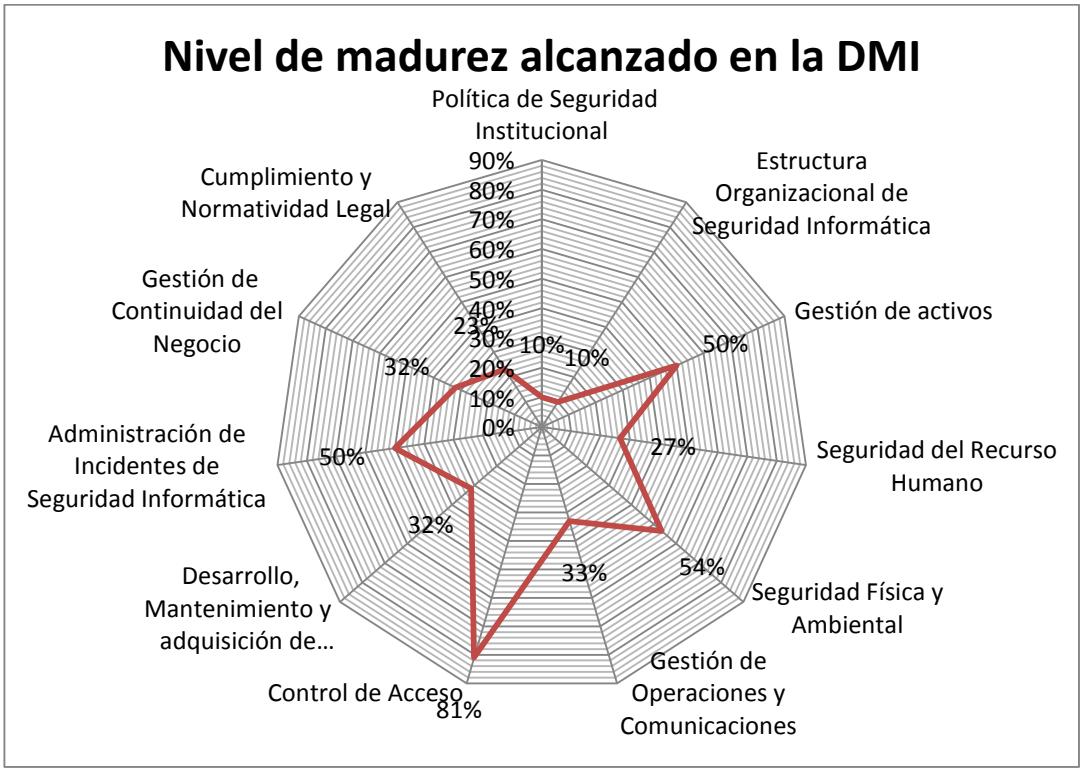

Figura 45. Nivel de madurez en la DMI, anexo 8

3.18 Conclusiones

La Dirección Metropolitana de Informática realiza esfuerzos aislados por hacer uso de los niveles de seguridad sobre los servicios o plataformas, pero mantiene una perspectiva del logro de metas y objetivos apoyados en la alta directiva permiten a la Dependencia implementar prácticas básicas de seguridad en las áreas de tecnología con un responsable en cada área.

La DMI no realiza ciclos periódicos de monitoreo, seguimiento de controles de seguridad para verificar su cumplimiento, situación evidenciada con las entrevistas al personal de las diferentes áreas, cuyos criterios son dispares en relación con la sensibilidad, importancia en el uso inadecuado de la información.

No se dispone de un procedimiento apropiado en el cual se puede identificar, analizar, evaluar, monitorear y revisar periódicamente los riesgos.

El procedimiento para una recuperación ante eventos de desastre es básico ya que carece de procesos y fases documentadas, informadas y probadas así como un sitio alterno.

Las áreas críticas identificadas de mayor riesgo son : Producción e Ingeniería de soluciones debido a la falta de criterio técnico en la aplicación de cambios en el software, así como la actualización en los sistemas en producción; los riesgos se incrementan con la inexistencia de un área de seguridad de la información que soporte la gestión de la seguridad.

El control de calidad de las aplicaciones es crítico, en vista que no se aplica ningún tipo de evaluación en las fases de mantenimiento, pruebas y liberación, lo que evidencia altos niveles de riesgos en las aplicaciones que actualmente dar servicio a la ciudadanía así como a las áreas de la municipalidad.

Como se muestra en la Figura 45, la brecha mas critica es la Politica de Seguridad institucional en la que se deberá enfocar esfuerzos que equilibren un modelo o sistema de gestion de la seguridad equilibrado.

Los hallazgos comentados, evidencian la necesidad de tomar acciones correctivas que permitan aumentar el nivel de confianza de las operaciones ejecutadas por las DMI, en este sentido, es recomendable implementar un modelo de

control y evaluación de seguridad, que cimente su diseño en un conjunto de controles, normas internacionales de seguridad. En el capítulo IV se detalla la propuesta de diseño del modelo y las actividades para su aplicación.

CAPITULO IV

4 Modelo

4.1 Planteamiento

La institución presenta como recurso institucional a la información el cual es un insumo para la toma de decisiones por parte de la alta directiva, para garantizar la continuidad del servicio el cual es controlado y monitoreado siendo éste el Core de la Institución.

El presente modelo se sustenta en diseño de experimentos en el cual se va a decidir el mejor tratamiento para el control de las políticas de Gestión las cuales influyen en las áreas de TI de la DMI. El esquema reside en un aspecto de monitoreo, control y práctico el cual está estructura en las siguientes fases:

- Diagnóstico
- Desarrollo
- Experimentos
- Diseño del modelo (ESQUEMA)

Diagnóstico.- Esta fase está diseñada para determinar las variables a ser utilizadas luego de haber realizado el estudio en campo a la DMI y dependencias desconcentradas.

Desarrollo.- En esta fase se toma como requisitos los resultados obtenidos del diagnóstico para identificar las variables que apoyarán al desarrollo del Modelo de Control y Evaluación, considerando como elementos primordiales los controles de las normas y estándares internacionales enfocados a mantener la seguridad de la información no solo a nivel directivo, sino a nivel de cada área.

Experimentaciones.- En esta fase se realizó pruebas de comportamiento del modelo de control frente a los controles de la norma internacional de la ISO 27002.

Metodología de implementación.- En esta fase se determina la metodología para que el personal designado por la institución, implemente el modelo el cual va a permitir disminuir el riesgo.

4.1.1 Diagnóstico

El modelo está formado por un conjunto de variables obtenidas del diagnóstico realizado a las áreas de tecnología que mantiene la Institución, con el objetivo de minimizar el riesgo que constantemente afecta a la tecnología, el control tiene tres momentos importantes que se presenta de la siguiente forma: antes del control, en la implementación del control y después de la implementación en el control, en el capítulo anterior se trató del diagnóstico en la cual se realizó un levantamiento de información para determinar las vulnerabilidades existentes, sobre los departamentos que conforman el área de tecnología de la DMI, de ésta forma se pueden identificar insumos que están encaminadas a detectar, tratar y disminuir vulnerabilidades.

En el proceso de identificación de variables para el modelo, se ha visto necesario que pase por un proceso de experimentación, con el fin de obtener datos reales a los cuales se analiza de forma objetiva. Es por eso que en este capítulo se hace mención al diseño de experimentos de forma que los cálculos se respalden por un método científico y/o estadístico.

Para la experimentación se toma como base la planeación del trabajo descrita en el capítulo IV de la Tesis, en el cual se presenta el diseño del experimento en la Tabla 33.

Tabla 34

Planiacion del trabajo para el diseño de la experimentación

ETAPA	CONCEPTO
Planeación	Se plantea como problema el desconocer si los controles existentes actúan como un factor importante que controle el riesgo.
Hipótesis	Determinar si el modelo de control y evaluación va a disminuir los niveles de riesgo de los controles en la mayoría de los casos tecnológicos establecidos por la DMI en el MDMQ.
Variables independientes	Representa a los indicadores de evaluación que actúan para evaluar el control.
Tratamientos	Utilizar los resultados obtenidos del estudio realizado en campo respecto al nivel de madurez que mantiene la DMI,a través del cual se identificaron los puntos vulnerables en los cuales la amenaza es más latente y está cerca del alcance para que la amenaza se materialice.
Muestras	Se realizaron como mínimo 33 iteraciones considerando las que tengan mayor relevancia, el cual consta en el archivo (experimentaciones.xls)
Variable Dependiente	Es el valor obtenido entre la variable independiente y el impacto que se dio al activo de la información.
Interpretación	Definir los dominios en porcentaje de criticidad para poner mayor control en menor tiempo.

4.1.2 Desarrollo

El desarrollo está basado en los resultados obtenidos de la tabulación de las encuestas, en la que se verificó el cumplimiento de las Política de Gestión Tecnológico y se determinó que la institución posee un alto grado de riesgo en la seguridad de la información.

Para realizar el análisis se desarrolló la matriz frente a los controles de la norma internacional ISO 27002, como se muestra en la Tabla 34, que presenta la siguiente información:

- ISO Ref: Determina el ítem del control de la ISO 27002.
- ISO Descripción: Determina el nombre del control de acuerdo a la ISO 27002
- Ítem de la Encuesta: Se detalla la inicial del área acompañada con el número de pregunta o "No aplica a la institución".
- Indicador: Representa al valor cuantitativo de las respuesta obtenida en la encuesta, tomando valores de 1(bajo riesgo) a 5 (alto riesgo) y N/A "No aplica".
- Impacto: Representa al valor cuantitativo de 1(bajo riesgo) a 5 (alto riesgo) que afecta al activo de la información de la institución, el mismo que se encuentra detallado en el anexo 10.

Tabla 35

Relación de los Controles de la ISO27002 con el detalle de las encuestas

ISO Ref.	ISO Descripción	ITEM DE LA ENCUESTA	Indicador	Impacto
5.- Política de Seguridad		no existe control	5	5
6.- Estructura Organizacional de Seguridad Informática		no existe control	5	5
7. - Gestión de activos				
7,1	Responsabilidad por Recursos Cítricos			
7.1.1	Inventario de activos tecnológicos	C12, C15	4	5

Continúa →

7.1.2	Responsables de los activos tecnológicos	C12, C15	4	5
7.1.3	Uso aceptable de los activos tecnológicos	C12, C15	4	5
7,2	Clasificación de la Información			
7.2.1	Normas para clasificación de la información	P11	1	3
7.2.2	Identificación y Manejo de la información	C3, C17	2	3
8.- Seguridad del Recurso Humano		no existe control	5	3
9.- Seguridad Física y Ambiental				
9,1	Áreas Restringidas			
9.1.1	Perímetro de Seguridad Física	P18	2	4
9.1.2	Controles físicos de entrada	P18	2	4
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	P17	2	4
9.1.4	Protección contra amenazas externas y ambientales	P38	2	4
9.1.5	Trabajo en áreas restringidas	P18	2	4
9.1.6	Acceso público, envíos y áreas de carga	no aplica a la institución	N/A	N/A
9,2	Seguridad de los Componentes Tecnológicos			
9.2.1	Ubicación y protección de equipos tecnológicos	R3	1	4
9.2.2	Seguridad en el suministro de electricidad	P36	1	5
9.2.3	Seguridad en el cableado	R18	1	5
9.2.4	Mantenimiento	P28, P34, P35	2	5
9.2.5	Seguridad de equipos fuera de las áreas seguras	C20	4	5
9.2.6	Destrucción y reutilización de equipos	no aplica a la institución	N/A	N/A
9.2.7	Extracción de activos informáticos	no aplica a la institución	N/A	N/A
10.- Gestión de comunicaciones y operaciones				
10,1	Procedimientos Operacionales y Responsabilidades			
10.1.1	Documentación de procesos operativos	C5,C9,C11,C16	2	4
10.1.2	Control de Cambios	C18, P33, R11, IS6	3	5

Continúa →

10.1.3	Segregación de funciones	no existe control	5	4
10.1.4	Separación de los ambientes de Desarrollo, prueba y producción	P21	2	4
0,2	Administración de Servicios de terceros	no aplica a la institución	N/A	N/A
10,3	Planeamiento y aceptación de sistemas			
10.3.1	Administración de la capacidad	IS2	3	5
10.3.2	Aceptación de sistemas	IS2	3	5
10,4	Protección contra código malicioso y móvil			
10.4.1	Controles contra código malicioso	P37	2	5
10.4.2	Controles contra código móvil	NO EXISTE	5	5
10,5	Copias de seguridad			
10.5.1	Respaldo de la información.	P1,P3,P6	2	5
10,6	Administración de la seguridad de la red			
10.6.1	Controles de la Red	R13	2	4
10.6.2	Seguridad de los Servicios de Red	R12	2	5
10,7	Manipulación de medios			
10.7.1	Administración de medios removibles	no aplica a la institución	N/A	N/A
10.7.2	Destrucción de medios	no aplica a la institución	N/A	N/A
10.7.3	Procedimientos de manejo de la información	P5,P7	3	2
10.7.4	Seguridad de la documentación de los sistemas	no existe control	5	5
10,8	Intercambio de información			
10.8.1	Políticas y procedimientos del intercambio de información	R19	1	5
10.8.2	Acuerdos para el intercambio	R20	3	5
10.8.3	Medios físicos en movimiento	no existe control	5	5
10.8.4	Mensajería Electrónica	C10	2	5
10.8.5	Sistemas de información de negocios	no aplica	N/A	N/A
10,9	Servicios de Comercio Electrónico			
10.9.1	Comercio Electrónico	no aplica	N/A	N/A
10.9.2	Transacciones en Línea	no existe	5	5
10.9.3	Información pública	no aplica	N/A	N/A

Continúa →

10.10	Monitoreo			
10.1.0.1	Auditoría de registros	no existe control	5	5
10.1.0.2	Uso de sistemas de monitoreo	R10	2	4
10.1.0.3	Protección de registros de monitoreo	C22	1	5
10.1.0.4	Registros de monitoreo de administradores y operadores	no existe control	5	5
10.1.0.5	Registro de fallas	no existe control	5	5
10.1.0.6	Sincronía	no existe control	5	4
11.- Control de Acceso				
11,1	Control de acceso a la información de acuerdo a las necesidades del negocio.			
11.1.1	Política de Control de Acceso	C2, C8	2	5
11,2	Administración de acceso de los usuarios			
11.2.1	Registro de Usuarios	P22	2	5
11.2.2	Administración de privilegios	P2, P4,P25, P29	2	5
11.2.3	Administración de Contraseñas	P23	1	5
11.2.4	Revisión de los permisos asignados a los usuarios	C1	1	5
11,3	Responsabilidades de los usuarios			
11.3.1	Uso de las contraseñas	P24	1	3
11.3.2	Equipos desatendidos	no existe control	5	5
11.3.3	Política de escritorios y pantallas limpias	no existe control	5	5
11,4	Control de acceso a la red de datos			
11.4.1	Políticas para el uso de los servicios de la red de datos	P9	2	5
11.4.2	Autenticación de usuarios para conexiones externas	R6	4	5
11.4.3	Identificación de equipos en la red	R9	1	3
11.4.4	Diagnóstico remoto y protección de la configuración de puertos	R7	4	5
11.4.5	Segregación en la red	no existe control	5	5
11.4.6	Control de conexión a la red	C19	4	4
11.4.7	Control de enrutamiento de la red	R5	4	5
11,5	Control de acceso a los sistemas operativos			

Continúa →

11.5.1	Procedimientos para inicio de sesión de las estaciones de trabajo	no existe control	5	3
11.5.2	Identificación y autenticación de los usuarios.	P26, P30	2	5
11.5.3	Sistema de administración de contraseñas.	no existe control	5	5
11.5.4	Uso de las utilidades del sistema	no existe control	5	5
11.5.5	Time-out para las estaciones de trabajo.	no existe control	5	5
11.5.6	Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	no existe control	5	5
11,6	control de acceso a las aplicaciones			
11.6.1	Restricción de acceso a los sistemas de información	no existe control	5	5
11.6.2	Aislamiento de sistemas sensibles	no existe control	5	5
11,7	Computación Móvil y Teletrabajo			
11.7.1	Computación Móvil y comunicaciones	R1,R4	2	5
11.7.2	Teletrabajo	no aplica		N/A
12.- Desarrollo, Mantenimiento y adquisición de Sistemas de Información				
12,1	Requerimientos de seguridad para los sistemas de información			
12.1.1	Análisis y especificaciones de los requerimientos de seguridad	P19	2	5
12,2	Procesamiento correcto en aplicaciones			
12.2.1	Validación de los datos de entrada	IS1	3	5
12.2.2	Control del procesamiento interno	P32	1	5
12.2.3	Integridad de los mensajes	no existe control	5	5
12.2.4	Validación de los datos de salida	no existe control	3	5
12,3	Controles Criptográficos			
12.3.1	Política para el uso de controles criptográficos	IS7	5	5
12.3.2	Administración de llaves	P31	1	5
12,4	Seguridad en los archivos del sistema (System Files)			
12.4.1	Control del software operacional	no existe control	5	3
12.4.2	Protección de los datos en sistemas de prueba	IS8	3	5

Continúa →

12.4.3	Control de acceso a las librerías de código fuente	no existe control	5	5
12,5	Seguridad en el desarrollo y en los procesos de soporte técnico			
12.5.1	Procedimientos para el control de cambios	P20	3	5
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	IS9	2	5
12.5.3	Restricciones a cambios en paquetes de software	IS3	4	5
12.5.4	Fuga de información	P8	2	4
12.5.5	Desarrollo de software por parte de Outsourcing	no aplica	N/A	N/A
12,6	administración técnica de vulnerabilidades			
12.6.1	Control técnico de vulnerabilidades	no existe control	5	5
13 - Administración de Incidentes de Seguridad Informática				
13,1	Reporte de eventos de seguridad informática y de sus debilidades			
13.1.1	Reporte de eventos de Seguridad de la información.	R8	2	3
13.1.2	Reporte de debilidades de seguridad	R17	1	5
13,2	Administración de incidentes de seguridad informática y de su mejoramiento			
13.2.1	Responsabilidades y procedimientos	R2	1	5
13.2.2	Aprendizaje a partir de los incidentes de seguridad	R15	4	5
13.2.3	Recolección de evidencia	R16	4	5
14. - Administración de Continuidad del Negocio				
14,1	Consideraciones para la administración de la continuidad del negocio			
14.1.1	Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio	P13	3	5
14.1.2	Continuidad del negocio y análisis de impacto	P15	3	5
14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la SI	P12	2	5
14.1.4	Marco de planeación para la continuidad del negocio	P14	4	5
14.1.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	P16	2	5

Continúa →

15 - Cumplimiento y Normatividad Legal				
15,1	Cumplimiento con requerimientos legales			
15.1.1	Identificación de leyes aplicables	IS4	2	2
15.1.2	Derechos de autor y propiedad intelectual	IS10	2	5
15.1.3	Salvaguardar los registros de la organización	P10	3	3
15.1.4	Protección de los datos y privacidad de la información personal	P27	2	5
15.1.5	Prevención mal uso de los componentes tecnológicos	R14, C23	1	4
15.1.6	Regulación de controles criptográficos	IS5	2	3
15,2	Revisión de la política de seguridad y cumplimiento técnico			
15.2.1	Cumplimiento del requerimiento y controles establecidos por la política de gestión	C14	2	5
15.2.2	Verificación del cumplimiento técnico	C4,C6,C7, C13	3	4
15,3	Consideraciones relacionadas con la auditoría interna			
15.3.1	Controles para auditoría del sistema	P39	5	5
15.3.2	Protección de las herramientas para auditoría del sistema	P40	5	5

Fuente: López & Lala, 2013, anexo 10

Para el desarrollo del modelo se utilizó como base los campos de Indicador e Impacto representados en la Tabla 34, en la que se evidenció diferentes valores en un rango de (1 a 5), por lo tanto, se utilizó como herramienta de apoyo la media ponderada((Calmaestra, 2005)), que permitió determinar el valor de impacto e Indicador por dominio.

La operatividad de la media ponderada en el modelo, se aplica con la siguiente ecuación:

$$MPD = \frac{\sum_{i=1}^{n} (\text{Indicador } i * \text{Impacto } j)}{n}$$

Ecuación 5, Media ponderada de los dominios.

Dónde:

- n = Representa el número de controles de cada dominio.

- i = Representa al número de controles de [1…n] que tienen el objetivo de control.
- j = Representan al impacto que se asignó al control actual.
- MPD: Representa a la media ponderada por dominio.

Con los valores obtenidos del Impacto e Indicador por dominio, se procedió a calcular el riesgo actual que presenta la institución para cada dominio, utilizando la siguiente ecuación:

Ecuación 6, Riesgo (27005:2012, 2012)

La tabla 35, detalla la línea de base de la madures de la DMI.

- El Impacto por dominio se obtiene del promedio de los impactos obtenidos para cada control.
- El Indicador por dominio se obtiene de la media ponderada del impacto y el indicador de cada control.
- El riesgo % es el valor del porcentual del riesgo de cada dominio.

Tabla 36

Cuadro estadístico de la Línea Base del Riesgo tecnológico de la institución

Dominio de la ISO 27002	Impacto por dominio	Indicador por dominio	Riesgo	Riesgo %
1.- Política de Seguridad	5,00	5,00	25,00	100,00
2.- Estructura Organizacional de Seguridad Informática	5,00	5,00	25,00	100,00
3. - Gestión de activos	4,20	2,93	12,30	49,20
4.- Seguridad del Recurso Humano	3,00	4,44	13,33	53,33
5.- Seguridad Física y Ambiental	4,37	2,14	9,33	37,33
6.- Gestión de comunicaciones y operaciones	4,63	3,12	14,44	57,78
7.- Control de Acceso	4,71	3,42	16,13	64,50
8.- Desarrollo, Mantenimiento y adquisición de Sistemas de Información	4,80	3,24	15,53	62,13
9 - Administración de Incidentes de Seguridad Informática	4,60	3,00	13,80	55,20

Continúa →

10. - Administración de Continuidad del Negocio	5,00	2,80	14,00	56,00
11 - Cumplimiento y Normatividad Legal	4,10	3,09	12,67	50,67
Riesgo total				**60,44 %**

Fuente: López & Lala, 2013, anexo 8

De acuerdo a los resultados obtenidos en la Tabla 36, se procede a utilizar la fórmula de la media simple, de ésta manera se obtiene el riesgo total de tecnología que presenta la Dirección Metropolitana de Informática, para lo cual la ecuación es la siguiente:

$$RT \text{ (Riesgo total)} = (\sum (\text{riesgo})) / \ n$$

Figura 46, Riesgo total bajo la ISO 27002

Donde

- n - Es el número de dominios

El resultado es equivalente al porcentaje de ítems de los dominios, y se usa para calificar el nivel de riesgo de la siguiente forma: Alto (80 a 100%), medio alto (60 a 80%), medio (40 a 60%), medio bajo (20 a 40%) y bajo (0 a 20%); por lo tanto, el riesgo total que presenta la institución es de **60,44% equivalente a riesgo medio alto.**

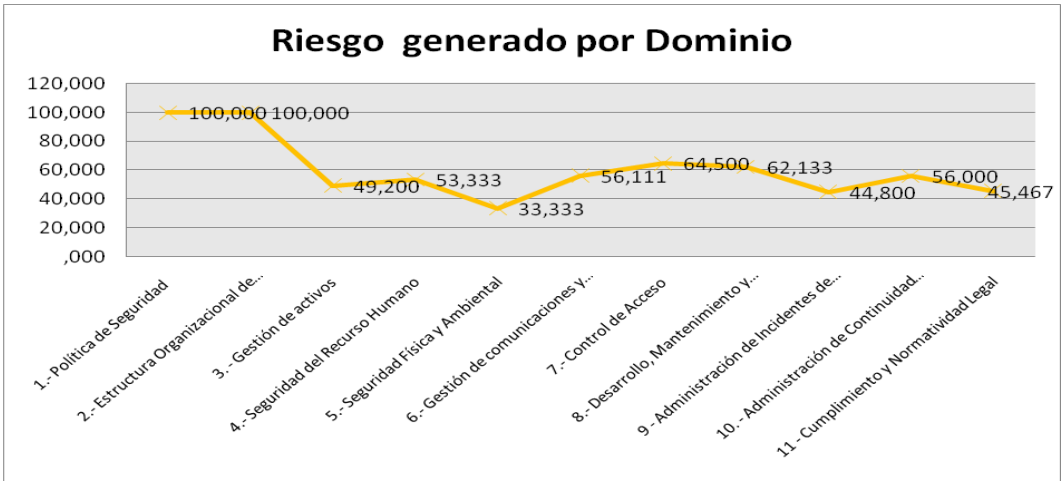

Figura 47. Riesgo obtenido por Dominio de la ISO 27002, anexo 9.

En la figura 47, se visualiza la línea base del riesgo actual que presenta la institución, por cada dominio.

4.1.3 Experimentación

En esta fase se realizó la experimentación para observar el comportamiento del riesgo tecnológico total de la DMI, utilizando valores de exposición en cada control del dominio, tales como:

- 1= control óptimo.
- 3= Control medio
- 5= no existe control.

El objetivo general de la experimentación es diseñar un modelo que permita implementar la evaluación de la política de gestión tecnológica apoyándose en el estándar de la ISO/ IEC 27002. Para lo cual se determinó un conjunto de dominios que luego de la experimentación se evidenció que se puede aplicar control que puedan minimizar el riesgo, los dominios son (d1, d2, d4, d6, d7, d8, d9, d11); y están relacionados con controles que no son óptimos y que actualmente está aplicando la institución y en otros casos no existe controles de seguridad.

De acuerdo al análisis se determinó realizar 33 experimentos agrupados por dominio, tomando como referente los valores de control alto (5), medio (3) y bajo (1) para observar el comportamiento de la variación del riesgo en cada dominio de la ISO 27002.

A continuación se detalla los experimentos realizados a cada dominio, para lo cual se hace uso de los siguientes campos:

- Dominio.- Representa al dominio de la ISO 27002.
- Impacto por dominio.- Es el valor promedio del dominio
- InD.- Representa al valor de exposición del dominio que determina su comportamiento.
- R.- Representa al valor del riesgo por dominio
- RP.- Representa al valor de riesgo porcentual.

Experimento 1: Se realizó al Dominio de la Política de Seguridad, el cual presenta un riesgo identificado de 100% equivalente a un riesgo alto; en la tabla 37, se puede observar que el riesgo del dominio cambia en los diferentes escenarios.

Tabla 37

Primer experimento en el Dominio Política de Seguridad.

Experimento N° 1													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
1.- Política de Seguridad	5	5	25	100	1	5	20	3	15	60	5	25	100

Riesgo por nivel de exposición	
Línea Base	60,44%
Al minimizar	53,17%
Medio	56,81%
Al maximizar	60,44%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 1, varían el riesgo total, puesto que al cambiar el valor del nivel de exposición da como resultado lo siguiente: (Ver Figura

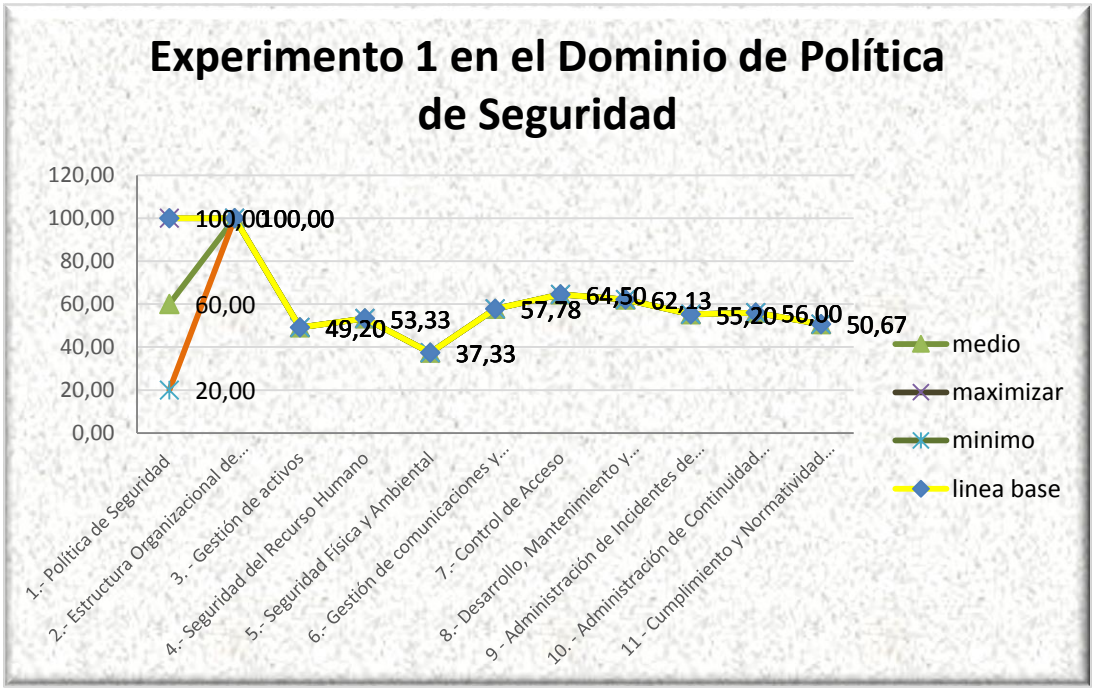

Figura 48, Experimento 1 en el Dominio de Política de Seguridad, anexo 9.

- Al poner en el nivel de exposición el valor de 1, el resultado del riesgo total disminuye a 53,17%; equivalente a un riesgo medio.
- Al poner en el nivel de exposición el valor de 3, el resultado del riesgo total disminuye a 56,18%; manteniéndose en un riesgo medio.

- Al no implementar controles y en el nivel de exposición poner el valor de 5, el riesgo total se mantiene con el mismo valor de la línea base.

Gráficamente en la Figura N° 48, presente a la línea base del riesgo intersecando con los valores de exposición alto, medio y bajo, en el cual se puede observar que con la generación, difusión, ejecución y monitoreo de políticas de seguridad alineadas a la necesidad de la institución va a existir mayor control y se bajaría el riesgo.

Experimento 2

El experimento 2 se realizó al Dominio de la Estructura Organizacional de Seguridad Informática, el cual presenta un riesgo en el dominio del 100%, en la tabla N° 38, se puede observar que el riesgo del dominio cambia en los diferentes escenarios.

Tabla 38

Experimento 2 al Dominio Estructura Organizacional de Seguridad Informática

Experimento 2													
		Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
Dominio	Impacto por Dominio	InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
2.- Estructura Organizacional de SI	5	5	25	100	1	5	20	3	15	60	5	25	100

Riesgo total	
Línea Base	60,44%
Al minimizar	53,17%
Medio	56,81%
Al maximizar	60,44%

Fuente: López & Lala, 2013, anexo 9

Como se puede observar en la tabla N° 37, los resultados obtenidos en el experimento 2 respecto al riesgo total no varían y son idénticos al experimento 1, lo que implica que para aumentar control debe existir recurso humano dentro de la estructura organizacional del SI.

Gráficamente se presenta la línea base cruzando con los valores del riesgo del dominio al minimizar, maximizar y poner valor neutral. Ver Figura N° 49

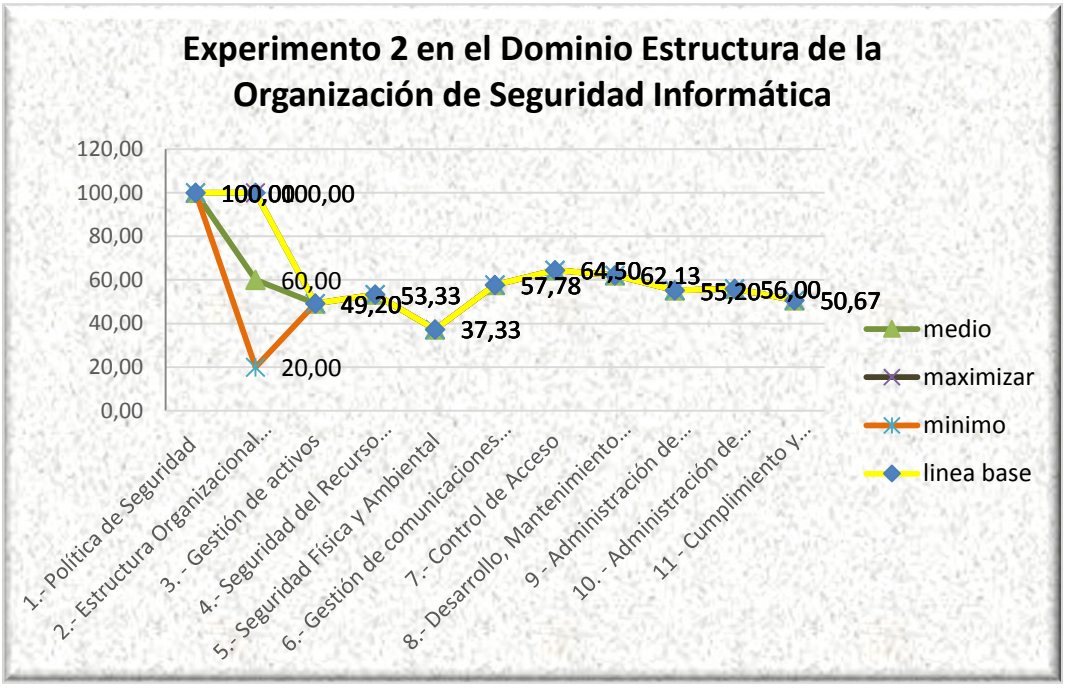

Figura 49, Experimento 2 en el Dominio de Estructura de la Organización de Seguridad Informática, anexo 9.

Experimento 3

El experimento 3 es realizado al Dominio Gestión de activos, el cual presenta como riesgo actual de dominio del 49,20%, equivalente a un riesgo medio bajo; en la tabla N° 39, se puede observar que el riesgo varía en los diferentes escenarios.

Tabla 39

Experimento 2 en el Dominio de Gestión de Activos

Experimento 3													
		Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
Dominio	Impacto por Dominio	InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
3.- Gestión de activos	4,20	2,93	12,3	49,20	1	4,0	16,80	3	12,6	50,40	5	21	84

Riesgo total		
	Línea Base	60,44%
	minimizar	57,50%
	Medio	60,55%
	Al maximizar	63,61%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 3, varían en el riesgo total en los tres escenarios dando como resultado la siguiente información:

- Al poner en el valor de exposición el dato de 1, el valor del riego por dominio disminuye a 16,80 % equivalente a un riesgo bajo, el cual es óptimo para el modelo.
- Al poner en el valor de exposición el dato de 3 o 5, el valor del riesgo total y por dominio aumento lo que implica que estos valores no son óptimos para el desarrollo del modelo.

Gráficamente se observa que el valor de exposición de 1 es óptimo para ser parte del modelo. Ver Figura N° 50.

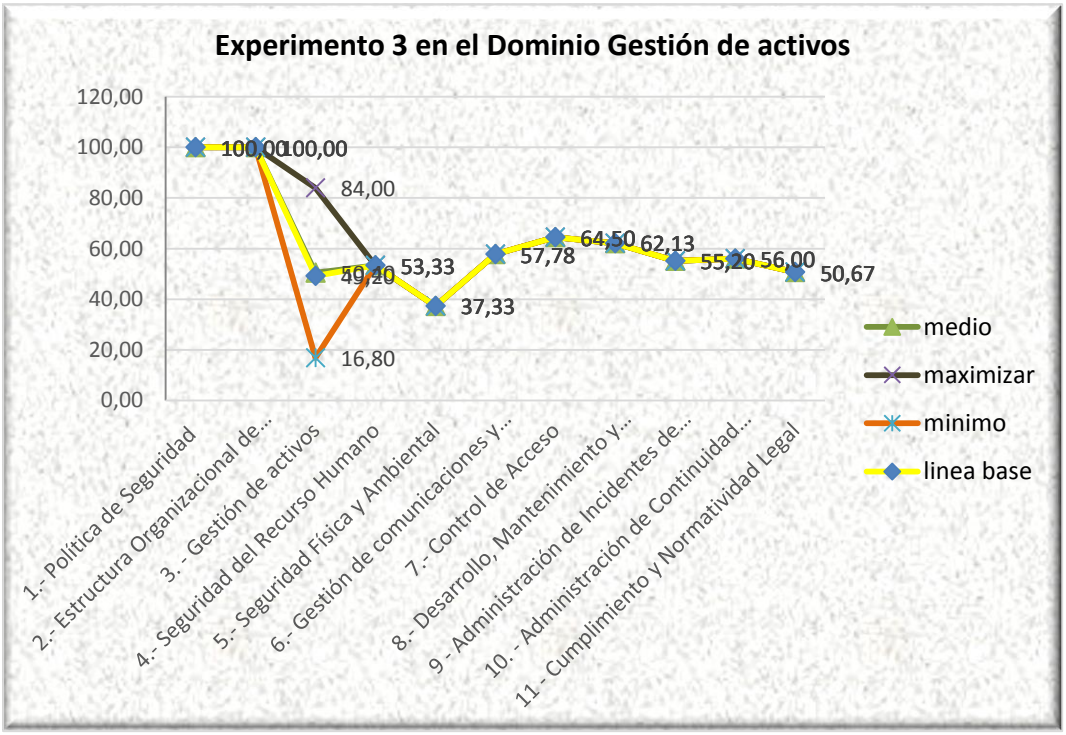

Figura 50, Experimento 3 en el Dominio de Gestión de activos, anexo 9.

Experimento 4

El experimento 4 es realizado al Dominio de Seguridad del Recurso Humano, el cual presenta como riesgo actual de dominio al 53,33% equivalente a un riesgo medio; en la Tabla N° 39, se puede observar la variación del riesgo porcentual en los diferentes escenarios.

Tabla 40

Experimento 4 en el Dominio de Seguridad de Recurso Humano

Experimento 4													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
4.- Seguridad de Recurso Humano	3	4,44	13,3	53,33	1	3	12	3	9	36	5	15	60

Riesgo total		
	Línea Base	60,44%
	Al minimizar	56,69%
	Medio	58,87%
	Al maximizar	61,05%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 4, se puede observar que existe variación el riesgo del dominio dando como resultado lo siguiente:

- Al poner en el valor de exposición el dato de 1, presenta como resultado en el riesgo por dominio de 12% equivalente a un riesgo bajo, el cual es óptimo para el desarrollo del modelo ya que permite disminuir el riesgo total de 56,69%.

- Al poner en el valor de exposición el dato de 3, presenta como resultado un riesgo bajo del 36% y de la misma forma es óptimo para el modelo ya que disminuye el valor total del riesgo a 58,87%.

- Al poner en el valor de exposición el dato de 5, presenta como resultado un riesgo alto por dominio de 60%, el cual no es óptimo para el modelo porque aumenta el riesgo total de la institución.

Gráficamente se puede observar que con el valor de exposición óptimo a aplicarse en el modelo es 1 o 3 ya que con éstos valores me permite minimizar el riesgo total de tecnología. Ver Figura N° 51.

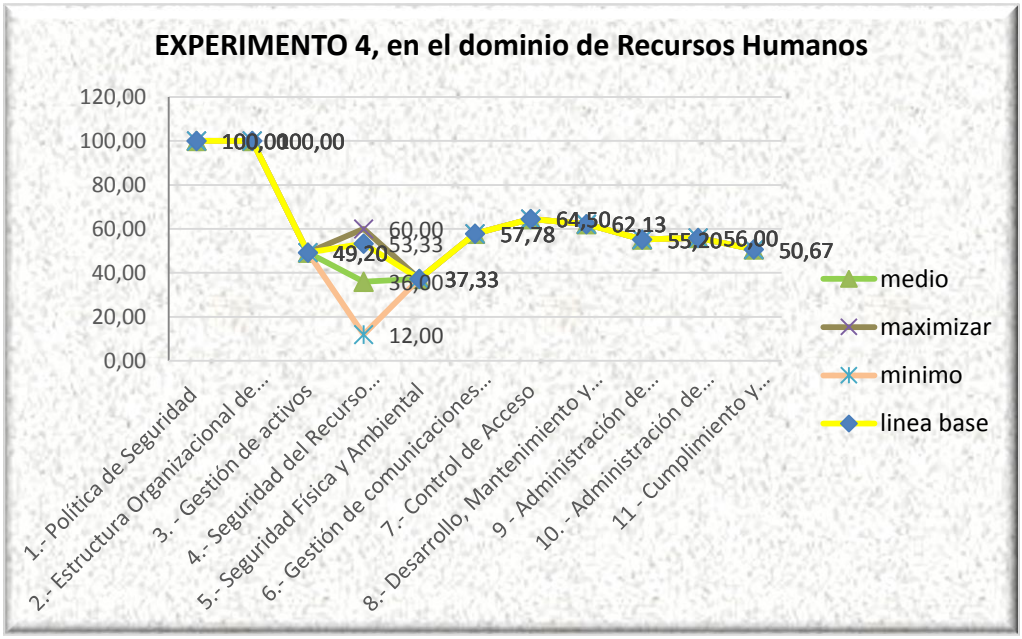

Figura 51, Experimento 4 en el Dominio de Seguridad del Recurso Humano, anexo 9

Experimento 5

El experimento 5 se realizó al Dominio de Seguridad Física y Ambiental, el cual presenta como riesgo de dominio al 33,33% equivalente a un riesgo medio bajo; en la tabla N° 40 se puede apreciar la variación en el campo de riesgo porcentual en los diferentes escenarios.

Tabla 41, Experimento 5 en el Dominio de Seguridad Física y Ambiental

Experimento 5 en el Dominio de Seguridad Física y Ambiental

Experimento 5													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
5.- Seguridad Física y Ambiental	4,37	1,91	8,33	33,33	1	4,37	17,47	3	13,1	52,4	5	21,8	87,33

Riesgo total		
	Línea Base	60,44%
	Al minimizar	59,00%
	Medio	62,18%
	Al maximizar	65,35%

Fuente: López & Lala, 2013, anexo 9

En los resultados obtenidos en el experimento 5, se puede observar que existe variación en el riesgo del dominio, como se detalla a continuación:

- Al poner en el valor de exposición el dato de 1, el riesgo del dominio disminuye al 17% teniendo como resultado un riesgo total bajo del 59%, lo que representa como un dato óptimo para el modelo.
- Al poner en el valor de exposición el dato de 3, el riesgo del dominio aumenta al 52,4%, lo que genera que el riesgo total de la institución aumente al 62,18% el cual no es óptimo para nuestro modelo.
- Al realizar la experimentación con un valor de exposición de 5, el riesgo del dominio aumenta a un 87,33%, incremente el riesgo total, por lo tanto este dato no es utilizado en el desarrollo del modelo.

Gráficamente se observa que al poner en el valor de exposición el dato 1(máximo control), el riesgo por dominio y riesgo total disminuye siendo óptimo para el modelo. Ver Figura N° 52.

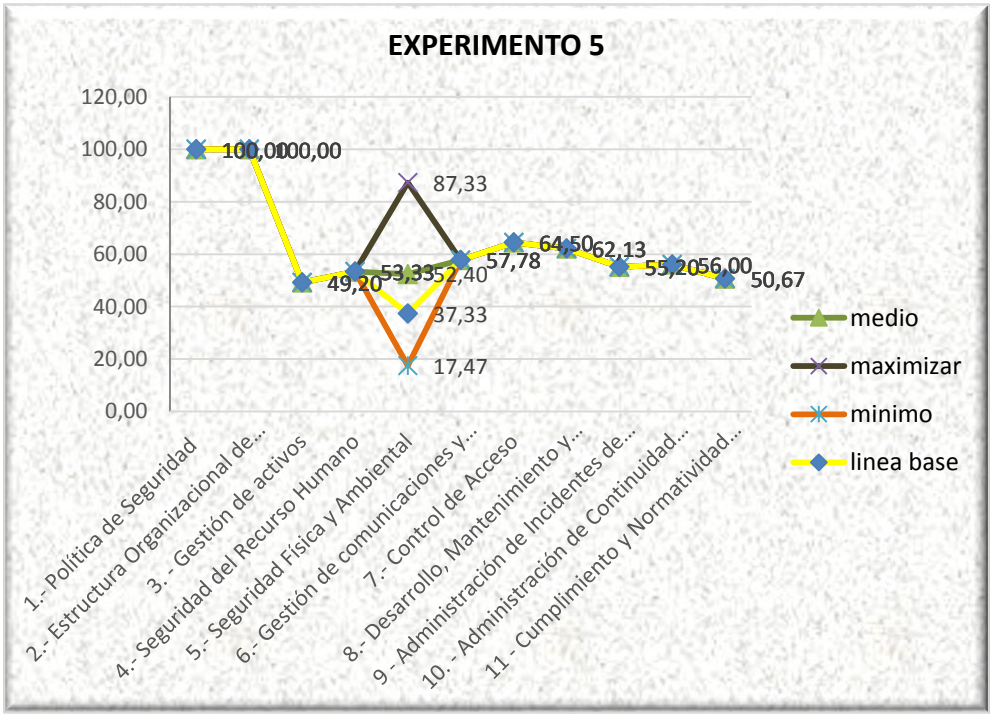

Figura 52, Experimento 5 en el Dominio de Seguridad Física y Ambiental, anexo 9.

Experimento 6

El experimento 6 se realizó al Dominio de Gestión de Comunicaciones y Operaciones, el cual presenta un riesgo por dominio del 56,11% equivalente a un riesgo medio; en la tabla N° 42 se puede apreciar la variación en el campo de riesgo porcentual en los diferentes escenarios.

Tabla 42

Experimento 6 en el Dominio de Gestión de Comunicaciones y Operaciones

Experimento 6													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
6.- Dominio de Gestión de Comunicaciones	4,63	3,03	14,0	56,11	1	4,63	18,5	3	13,88	55,5	5	23,1	92,5

Riesgo total		
	Línea Base	60,44%
	Al minimizar	57,02%
	Medio	60,39%
	Al maximizar	63,75%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 6, se observa que al cambiar el nivel de exposición, varía el riesgo del dominio como se detalla a continuación:

- Al poner en el nivel de exposición el valor de 1, el riesgo del dominio disminuye al 18,5 % lo cual es óptimo para el proyecto porque el riesgo total disminuye en un 57,02%.

- Al poner en el nivel de exposición el valor de 3, el riesgo del dominio se disminuye al 55,5%, el cual no es representativo para disminuir el riesgo total, pero formaría parte del modelo.
- Al poner en el nivel de exposición el valor de 5, el riesgo del dominio aumenta al 92,5% lo cual no es óptimo para el modelo porque el riesgo total incrementa en un 63,75%.

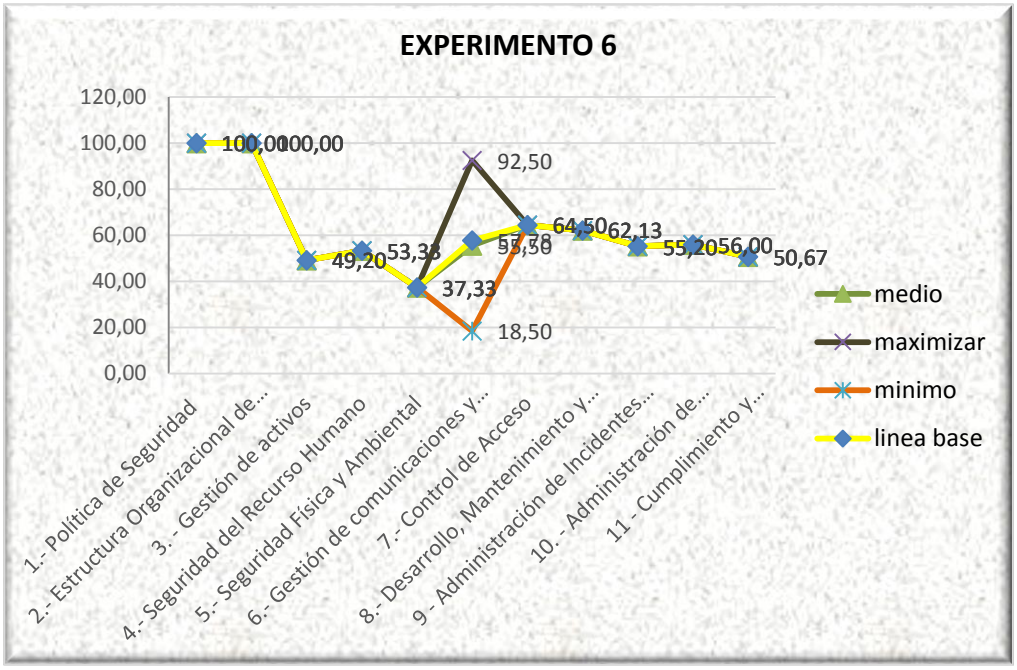

Figura 53, Experimento 6 en el Dominio de Gestión de Comunicaciones y Operaciones, anexo 9.

Gráficamente se observa que al poner los valores de 1 o 3 en los niveles de exposición, el riesgo total y por dominio disminuye. Ver Figura N° 53

Experimento 7

El experimento 7 se realizó al Dominio de Control de Acceso, el cual presenta un riesgo por dominio del 64,50%, equivalente a un riesgo medio alto; en la tabla N° 43 se puede observar que el valor porcentual varía en los 3 niveles de exposición.

Tabla 43

Experimento 7 en el Dominio de Control de Acceso

Experimento 7													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
7.- Dominio de Control de acceso	4,71	3,42	16,13	64,5	1	4,7	18,33	3	14,13	56,5	5	23,5	94,1

Riesgo total		
	Línea Base	60,44%
	Al minimizar	56,29%
	Medio	59,72%
	Al maximizar	63,14%

Fuente: López & Lala, 2013, anexo 9

Los resultados que presentan en el experimento 7, se observa que al cambiar el nivel de exposición, varía el riesgo porcentual del dominio, el mismo que se presenta a continuación:

- En el nivel de exposición cuando el valor es 1, el riesgo del dominio baja al 18,33%, siendo un dato óptimo para el modelo ya que el riesgo total baja a 56,29%.
- En el nivel de exposición cuando el valor es 3, el riesgo del dominio bajo, actuando éste valor como óptimo para el modelo ya que el promedio del riesgo total baja a 59,72% manteniéndose como riesgo medio.
- Al poner en el nivel de exposición el valor de 5, el riesgo del dominio aumenta considerablemente el cual no es considerado como muestra para el modelo.

Como resultado del experimento, el valor óptimo a utilizar en el nivel de exposición es de 1 o 3, gráficamente se presenta que a comparación de la línea base disminuye el riesgo. Ver Figura N° 54

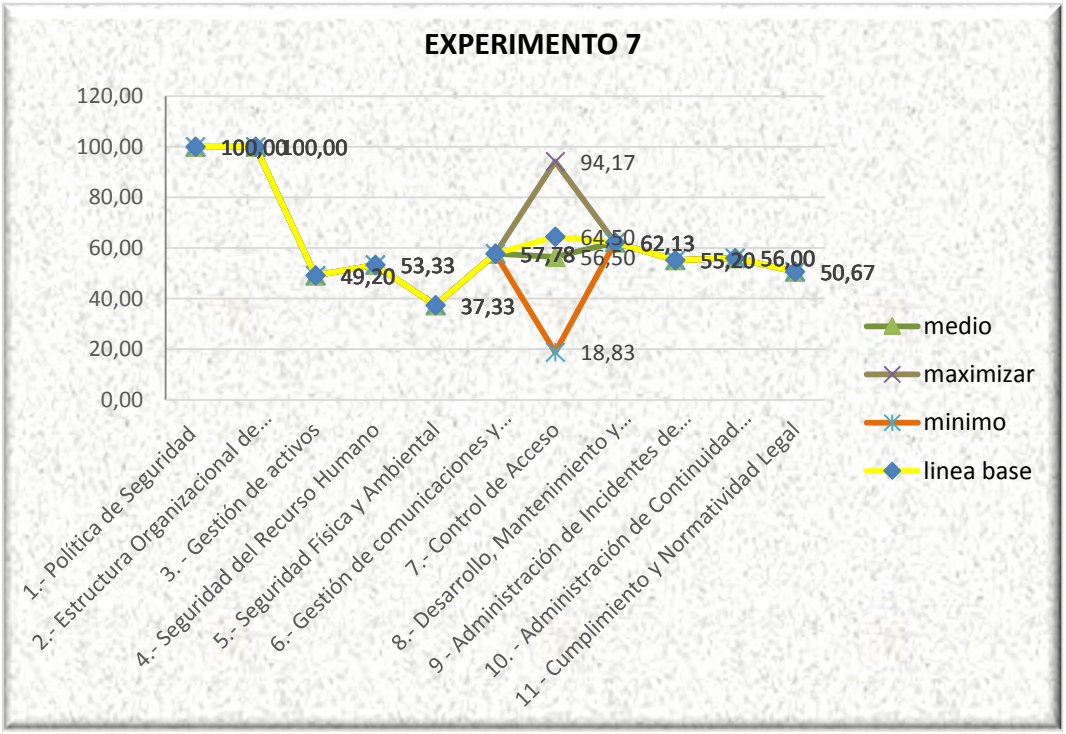

Figura 54, Experimento 7 en el Dominio de Control de Acceso, anexo 9

Experimento 8

El experimento 8 se realizó al Dominio de Desarrollo, Mantenimiento y adquisición de Sistemas de Información, el cual presenta como riesgo de dominio 62,13% equivalente a un riesgo medio alto; en la tabla N° 44, se observa que manteniendo como constante el valor del impacto del dominio, el valor porcentual en los 3 escenarios es diferente.

Tabla 44

Experimento 8 en el Dominio de Desarrollo, Mantenimiento y adquisición de SI

Experimento 8													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
8.- Desarrollo, Mantenimiento y adquisición de Sistemas de Información	4,8	3,24	15,53	62,13	1	4,8	19,2	3	14,4	57,6	5	24	96,0

Riesgo total		
	Línea Base	60,44%
	minimizar	56,54%
	Medio	60,03%
	Al maximizar	63,52%

Fuente: López & Lala, 2013, anexo 9

Los resultados que se obtuvieron en la experimentación N° 8, en los tres escenarios se detalla a continuación:

- En el nivel de exposición cuando el valor es de 1, el riesgo porcentual por dominio baja a 19,2%, actuando este como un valor óptimo para el modelo.
- En el nivel de exposición cuando el valor es de 3, el riesgo porcentual por dominio baja a 57,60% de la línea base, actuando este como valor óptimo para el modelo.
- En el nivel de exposición cuando el valor es de 5, el riesgo porcentual por dominio aumenta incrementando el riesgo al 96%.

Como resultado del experimento se determina que el valor óptimo del modelo es 1 o 3, actuando éstos como niveles de exposición, gráficamente se presenta que con el valor de exposición el riesgo disminuye de la línea base. Ver Figura N° 55

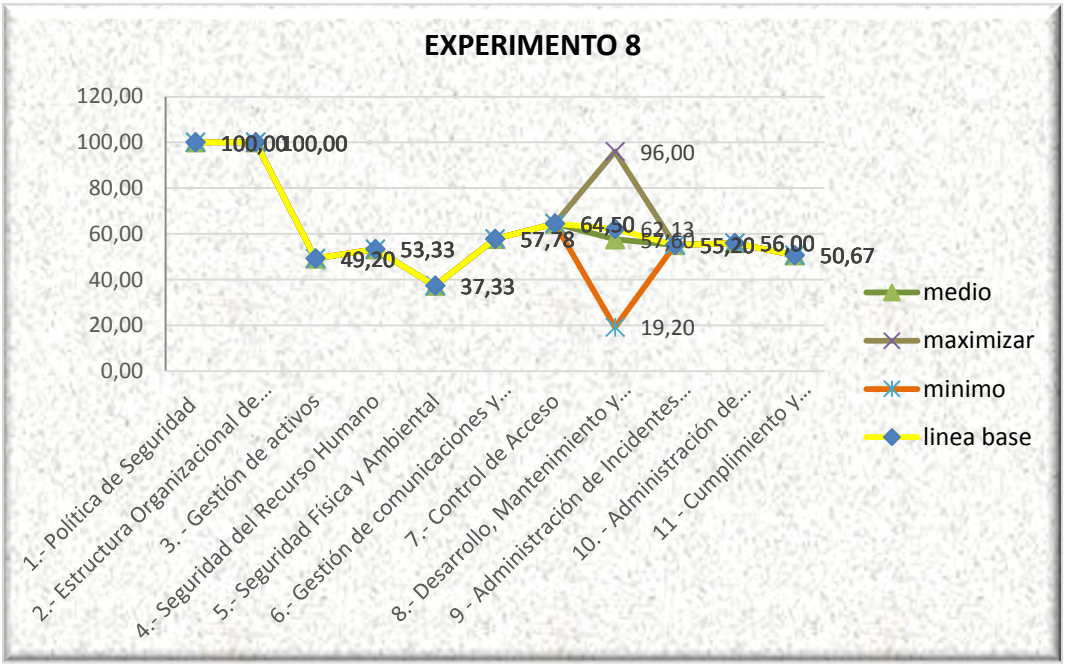

Figura 55, Experimento 8 en el Dominio de Desarrollo, Mantenimiento y adquisición de Sistemas de Información, anexo 9.

Experimento 9

El experimento 9 se realizó al Dominio de Administración de Incidentes de Seguridad Informática, el cual presenta como riesgo de dominio el 44,80% equivalente a un riesgo medio; en la tabla N° 45, se observa que el riego porcentual varía en los 3 escenarios.

Tabla 45

Experimento 9 en el Dominio de Administración de incidentes de seguridad

Experimento 9													
Dominio	Impacto por Dominio	Valores Línea Base			Valor de exposición= 1			Valor de exposición= 3			Valor de exposición= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
8.- Administración de Incidentes de Seguridad	4,6	2,43	11,2	44,8	1	4,6	18,4	3	13,8	55,2	5	23	92

Continúa →

esgo total	Línea Base	60,44%
	Al minimizar	58,04%
	Medio	61,39%
	A l maximizar	64,73%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 9, se observa que al cambiar el nivel de exposición, varía el riesgo del dominio como se detalla a continuación:

- En el nivel de exposición cuando el valor es de 1, el riesgo porcentual es bajo equivalente al 18,4%, de la misma manera disminuyendo el riesgo total a 58,04%.
- En el nivel de exposición cuando el valor es de 3 o 5, el riesgo porcentual está sobre la línea base, lo cual no representa como dato base para el modelo.

Como resultado del experimento se determina que el valor de exposición de 1 es óptimo, gráficamente se presenta que con el valor de exposición bajo, el riesgo disminuye de la línea base. Ver Figura N° 56

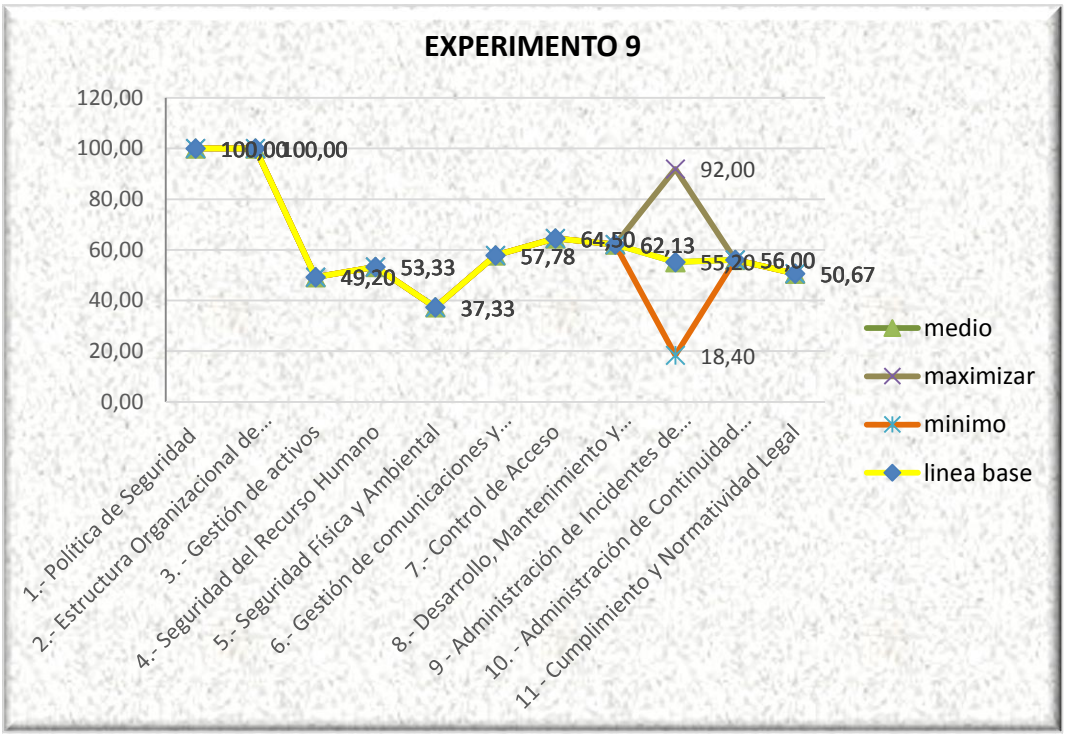

Figura 56, Experimento 9 en el Dominio de Administración de Incidentes de Seguridad, anexo 9

Experimento 10

El experimento 10 se realizó al Dominio de Administración de Continuidad del Negocio, el cual presenta como riesgo actual del dominio 56,00% equivalente a un riesgo medio; en la tabla N° 52 se presenta los diferentes niveles de exposición que permiten determinar la variación del riesgo del dominio.

Tabla 46

Experimento 10 en el Dominio de Administración de Continuidad del negocio

Experimento 10													
Dominio	Impacto por Dominio	Valores Línea Base			Minimizar Indicador= 1			Valor medio Indicador = 3			Valor alto Indicador= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
10.- Administración de Continuidad del Negocio	4,6	2,43	11,2	44,8	1	4,6	18,4	3	13,8	55,2	5	23	92

Riesgo total	
Línea Base	60,44%
Al minimizar	57,17%
Medio	60,81%
Al maximizar	64,44%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 10, varía el nivel de riesgo en los diferentes niveles de exposición, presentando como resultado lo siguiente:

- En el nivel de exposición con valor de 1, presenta un riesgo por dominio del 18,4% disminuyendo del riesgo de la línea base, actuando éste como un valor óptimo para el modelo.
- En el nivel de exposición con valor de 3 o 5, presentan un incremento en el riesgo del dominio aumentando el riesgo total que mantiene la institución, para el modelo estos valores no son óptimos.

En la experimentación 10, da como resultado que el valor de exposición de 1 es óptimo para el desarrollo del modelo, gráficamente se presenta que con el valor de exposición bajo, el riesgo disminuye de la línea base. Ver Figura N° 57

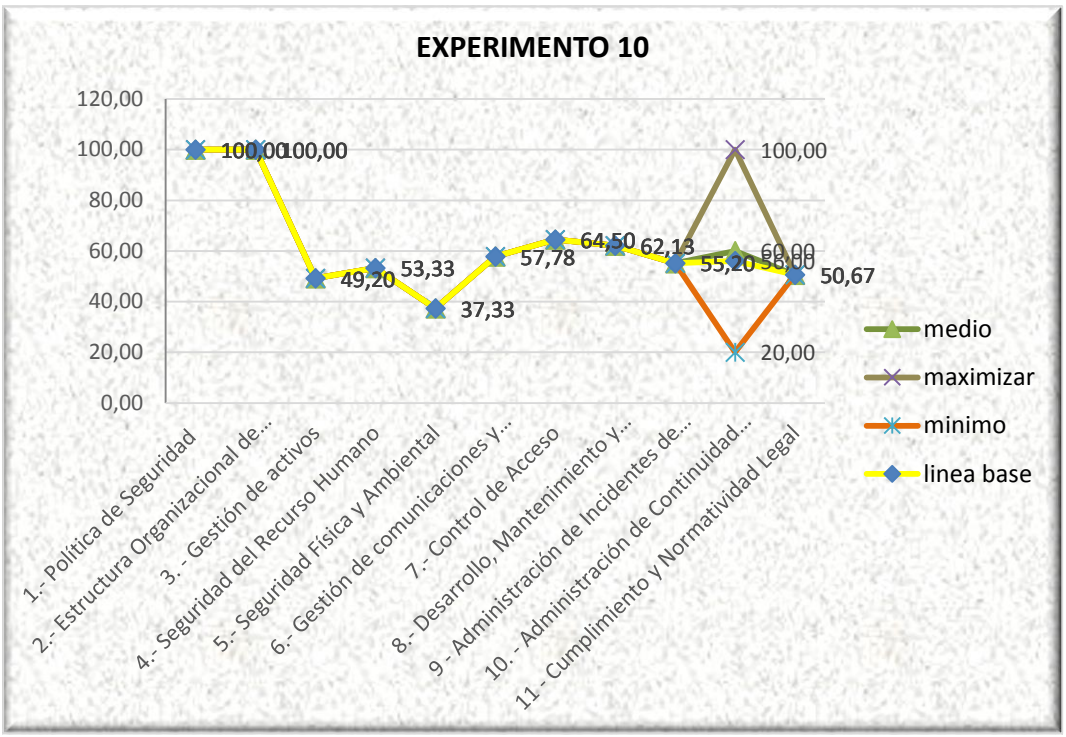

Figura 57, Experimento 10 en el Dominio de Administración de Incidentes de Seguridad, anexo 8.

Experimento 11

El experimento 11 se realizó al Dominio Cumplimiento y Normativa legal, el cual presenta como riesgo actual de dominio 45,47% equivalente a un riesgo medio; en la tabla N° 47 se observa que existe variación en los tres escenarios.

Tabla 47

Experimento 11 en el Cumplimiento y normativa legal

Experimento 11													
Dominio	Impacto por Dominio	Valores Línea Base			Minimizar Indicador= 1			Valor medio Indicador = 3			Valor alto Indicador= 5		
		InD	R	RP %	InD	R	RP %	InD	R	RP %	InD	R	RP %
11.- Cumplimiento y Normativa legal	4,1	2,77	11,4	45,47	1	4,1	16,4	3	12,3	49,2	5	20,5	82
Riesgo total					Línea Base					60,44%			
					Al minimizar					57,80%			

Continúa →

	Medio	60,78%
	Al maximizar	63,76%

Fuente: López & Lala, 2013, anexo 9

Los resultados obtenidos en el experimento 11, varía el nivel de riesgo presentando como resultado lo siguiente:

- En el nivel de exposición con valor de 1, presenta un riesgo por dominio del 16,4% disminuyendo del riesgo de la línea base, actuando éste como un valor óptimo para el modelo.
- En el nivel de exposición con valor de 3 o 5, presentan un incremento en el riesgo del dominio aumentando el riesgo total que mantiene la institución, para el modelo estos valores no son óptimos.

En la experimentación 11, da como resultado que el valor de exposición de 1 es óptimo para el desarrollo del modelo, gráficamente se presenta que con el valor de exposición bajo, el riesgo disminuye de la línea base. Ver Figura N° 58.

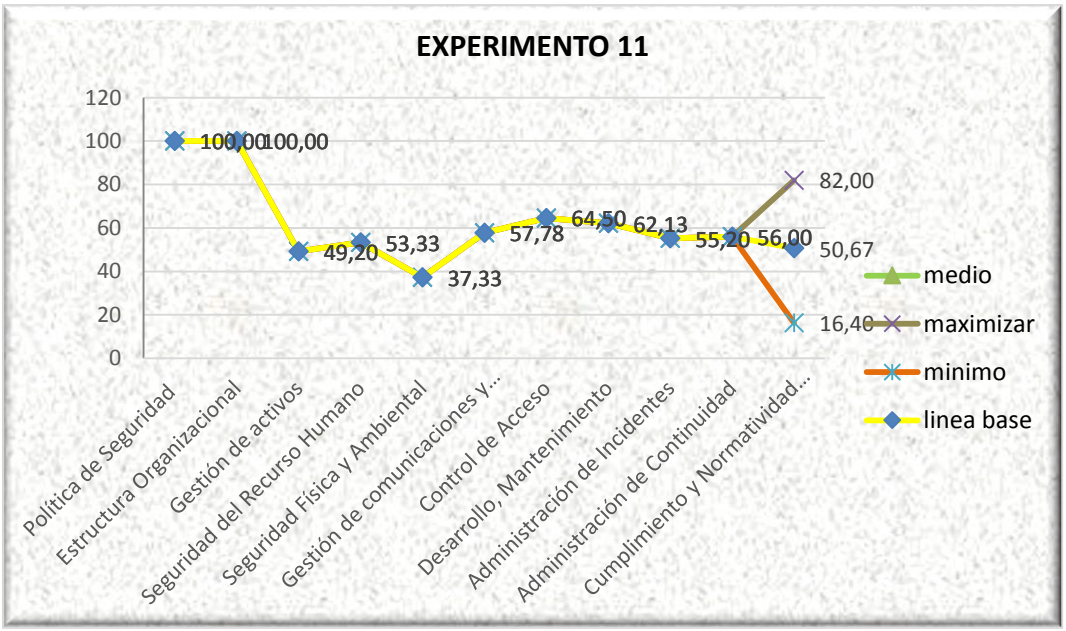

Figura 58, Experimento 10 en el Dominio de Cumplimiento y Normativa Legal, anexo 8.

Resultados

Una vez realizado los experimentos a los dominios de la ISO 27002 se encuentran en el ANEXO 8, utilizando como variable al nivel de exposición de 1= como máximo control, 3= como control medio o 5= no existe control, se determina que el riesgo por dominio, varía de la línea base en cualquier instancia.

Se puede apreciar en la tabla N° 48, los resultados obtenidos por dominio en cada uno de los experimentos, para determinar el modelo óptimo se selecciona el valor más bajo del riesgo obtenido en el experimento por dominio siempre que éste sea menor que el valor de la línea base.

Tabla 48

Cuadro estadístico que representa la Determinación del modelo de control

Dominio	Línea Base del Riesgo LB	Experimentos del riesgo por dominio E			Valores a ser tomados en el modelo	Modelo propuesto
		Riesgo bajo =1	Riesgo medio = 3	Riesgo alto = 5		
d1	100,0 %	20,0 %	60,0 %	100,0 %	(E=1 o E=3) < LB d1	Er:1 => 20,0 %
d2	100,0 %	20,0 %	60,0 %	100,0 %	(E=1 o E=3) < LB d2	Er=1 => 20,0 %
d3	49,2 %	16,8 %	50,4 %	84,0 %	(E=1 o E=3) < LB d3	Er=1 => 16,8%
d4	53,3 %	12,0 %	36,0 %	60,0 %	(E=1 o E=3) < LB d4	Er=1 => 12%
d5	37,3 %	17,5 %	52,4 %	87,3 %	(E=1) < LB d5	Er=1 => 17,5 %
d6	57,8 %	18,5 %	55,5 %	92,5 %	(E=1) < LB d6	Er=1 => 18,5 %
d7	64,5 %	18,8 %	56,5 %	94,2 %	(E=1 o E=3) < LB d7	Er=1 => 18,8 %
d8	62,1 %	19,2 %	57,8 %	96,0 %	(E=1 o E=3) < LB d8	Er=1 => 19,2 %
d9	55,2 %	18,4 %	55,2 %	92,0 %	(E=1) < LB d9	Er=1 => 18,4 %
d10	56,0 %	20,0 %	60,0 %	100,0 %	(E=1) < LB d10	Er=1 => 20 %
d11	50,7 %	16,4 %	49,2 %	82,0 %	(E=1 o E= 3) < LB d11	Er=1 => 16,4 %
Total de riesgo	62,38 %	18,0 %	53,9 %	89,8 %	E < RT	18,0 %
Desviación Estándar	19,9	2,34	7,03	11,70	E < RT	2,34

Continúa →

Coeficiente de Variación	**31,93%**	**13,03%**	**13,04%**	**13,03%**	**E < RT**	**13,03%**

Fuente: López & Lala, 2013, anexo 9

En la tabla N° 48, se propone el modelo con los 11 dominios de la ISO 27002, que va a permitir disminuir el riesgo actual de la institución, por lo tanto, para que el modelo sea óptimo el nivel de exposición tomaría el valor de 1 con un impacto de 3 a 5 el cual va a dar como resultado un riesgo bajo, en la Figura N° 59, se muestra el resultado de los experimentos en la cual la línea amarilla representa al riesgo alto, como se puede ver en la figura llega al nivel más alto del riesgo, lo que indica que al no tener controles que apoyen a la seguridad de la información afectaría a los activos que tiene la institución.

En contestación a la pregunta ***¿Cuál es la mejor solución que va a permitir a la Dirección Metropolitana de Informática, la implementación de controles proactivos en relación con las mejores prácticas de control interno basados en la normativa vigente?***

Una vez realizada la experimentación en el que se identificó que el riesgo existente en cada dominio de la norma ISO 27002 es alto y se propone un modelo que disminuya el riesgo como se muestra en la Figura N° 59, acercando más a 0 en el eje X.

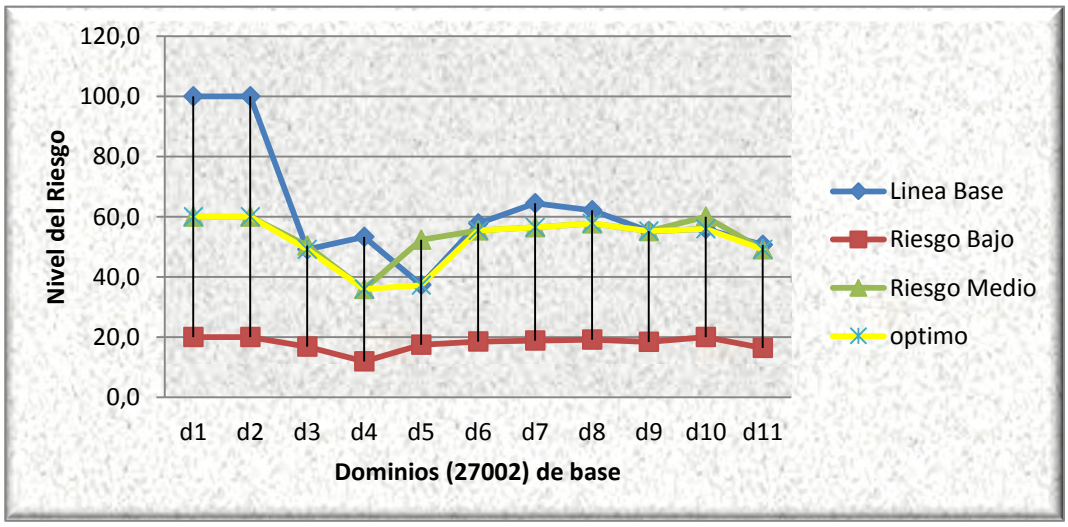

Figura 59, Estadística del resultado de los experimentos., anexo 9

En base a los resultados de las experimentaciones se propone mantener un control óptimo utilizando los dominios de la norma ISO 27002, y al ser implementados con el apoyo de la máxima autoridad de la institución, el riesgo disminuirá en cada dominio como se indica a continuación:

- En el dominio de Política de Seguridad, actualmente no se cuenta con controles por lo que se recomienda su implementación, que va a permitir disminuir el riesgo al 20%.

- En el dominio Estructura Organizacional de Seguridad, actualmente no se cuenta con controles por lo que se recomienda su implementación, que va a permitir disminuir el riesgo al 20%.

- En el dominio Gestión de activos se observa que actualmente la Dirección Metropolitana Informática mantiene control pero con el modelo se podría reducir a un 16,8% de riesgo.

- En el dominio Seguridad del Recurso Humano, actualmente se cuenta con controles cuyo valor es superior al valor medio, por lo que se recomienda implementar controles de ésta forma se tendría un riesgo aceptable del 12%.

- En el dominio Seguridad Física y Ambiental, se observa que actualmente presenta un riesgo medio aceptable pero con implementación de controles disminuiría el riesgo al 17,5% con la implementación de controles.

- En el dominio Gestión de comunicaciones y operaciones, actualmente se cuenta con controles cuyo valor es superior al modelo, por lo que se recomienda implementar controles, de ésta forma disminuir el riesgo al 18,5%.

- En el dominio Control de Acceso, actualmente se cuenta con pocos controles de acuerdo al modelo propuesto, por lo que se recomienda implementar controles disminuyendo el riesgo al 18,8%.

- En el dominio Desarrollo, Mantenimiento y adquisición de Sistemas de Información, actualmente presenta controles bajos, se recomienda implementar controles de ésta forma disminuir el riesgo del dominio en un 19,2%

- En el dominio Administración de Incidentes de Seguridad Informática se observa que existe un riesgo medio alto y con la implementación de controles disminuye el riesgo en un 20%.

- Para el dominio Administración de Continuidad del Negocio se observa que existe un riesgo medio alto y con la implementación de controles disminuye el riesgo en un 18,4%.

Para el dominio Cumplimiento y Normatividad Legal, actualmente se cuenta con bajos controles cuyo valor es superior al valor del modelo propuesto, por lo que se recomienda implementa controles para disminuir el riesgo al 16.4%.

Por lo tanto se puede determinar que el modelo propuesto va a permitir disminuir el riesgo total de 62,38% al 18%, obteniendo una distribución estándar del 2,34 obteniendo un modelo con datos menos dispersos y más homogéneos.

De tal forma al comparar la variabilidad del conjunto de datos entre la línea base y el modelo propuesto se determina que el menor coeficiente de variación equivalente a 13,033% indica que el modelo propuesto presenta una dispersión menor de sus controles lo que permite tener homogeneidad en los datos respecto a la variación del riesgo total equivalente a 31,937%, como se muestra en la Figura N° 60.

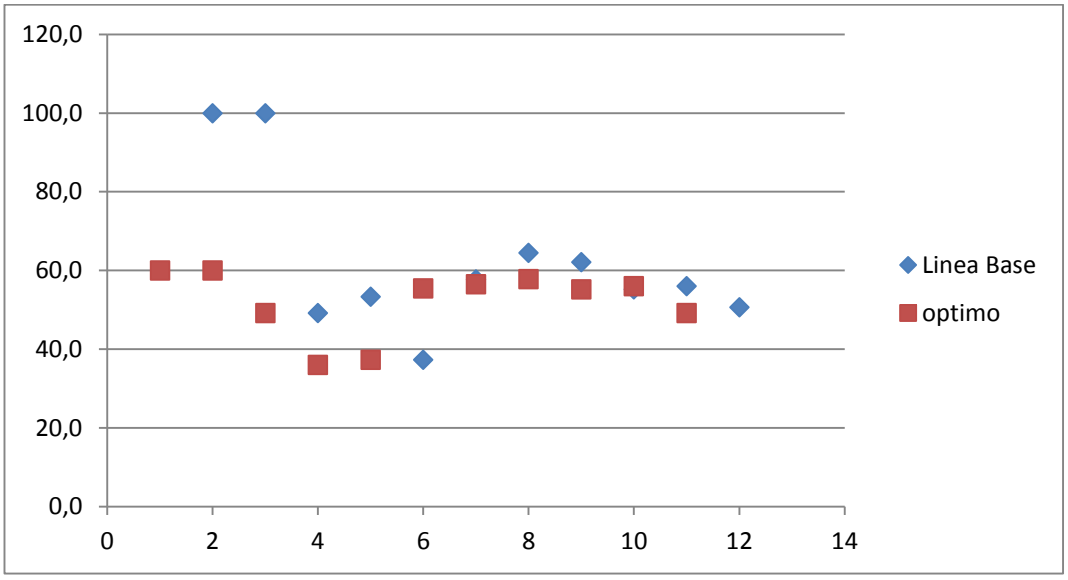

Figura 60, Dispersión de los Dominios, Anexo 9, Hoja "Resumen de pruebas"

4.1.4 Diseño del Modelo

De acuerdo al análisis realizado se detalla el modelo que va a permitir disminuir el riesgo, apoyada en la norma INEN ISO/IEC 27002, que enmarca la prioridad de algunas directrices que se alinean a la realidad institucional.

La implementación del modelo permitirá el incremento de controles en la seguridad de la información lo cual va a dar mayor confianza de los funcionarios que conforman el Municipio del Distrito Metropolitano de Quito.

Para lo cual se propone un modelo que permita mejorar, y actualizar la política de gestión tecnológica, por lo tanto, luego del análisis obtenido en la tabulación de las encuestas se ha evidenciado que existe un riesgo alto en temas de seguridad de la información, para lo cual se ha visto necesario apoyarse en la norma ISO 27002 la cual tiene como objetivo implementar controles de seguridad, por lo tanto, luego de realizar los experimentos implementando controles en los dominios se detectó que se puede minimizar el riesgo, aplicando la plantilla del ANEXO 11 que detalla los componentes a evaluarse.

Los objetivos planteados en el modelo son los siguientes:

- Mejorar los procesos de seguridad mediante cumplimiento de políticas para detectar y prevenir el riesgo.
- Evaluar los resultados obtenidos en el tema de seguridad con respecto a los controles implementados.
- Identificar nuevos controles para mejorar los procesos del dominio de la ISO 27002.

El alcance del modelo es evaluar la política de tecnología actual que utiliza la institución, y luego seleccionar la norma que permita alivianar la evaluación con el fin de que las instituciones puedan realizar un análisis de seguridad.

El modelo (Ver Figura 60), incluye los siguientes componentes:

- **Norma de Control (NC)**.- Norma o documento mandatorio que rige a la institución pública en temas de implementación de controles en el área de tecnología, los mismos que deben verse apoyados por su ente directivo.
- **Objetivo de evaluación (OE)**.- En el modelo está representado por los dominios que se detectaron a los cuales se les puede bajar el nivel de riesgo, éste a su vez está relacionado con los resultados obtenidos de las encuestas.
- **Definir medida de evaluación (ME)**.- Depende de la importancia que se quiera dar a los ítems del Objetivo de seguridad, se establece una directriz con un peso específico para cada ítem que permita generar un valor de calificación.
- **Proceso de evaluación(PE)**.- Describe el conjunto de actividades para comparar el objetivo de evaluación, al cual se le aplica una directriz de medida esto es en base a las especificaciones del entorno tecnológico, requerimientos y niveles de seguridad.
- Resultado de evaluación (RE).- De acuerdo a los ítems de los objetivos de seguridad y la medida de evaluación, se presentan resultados de evaluación cuantitativo que permite establecer y evaluar a la política de tecnología.

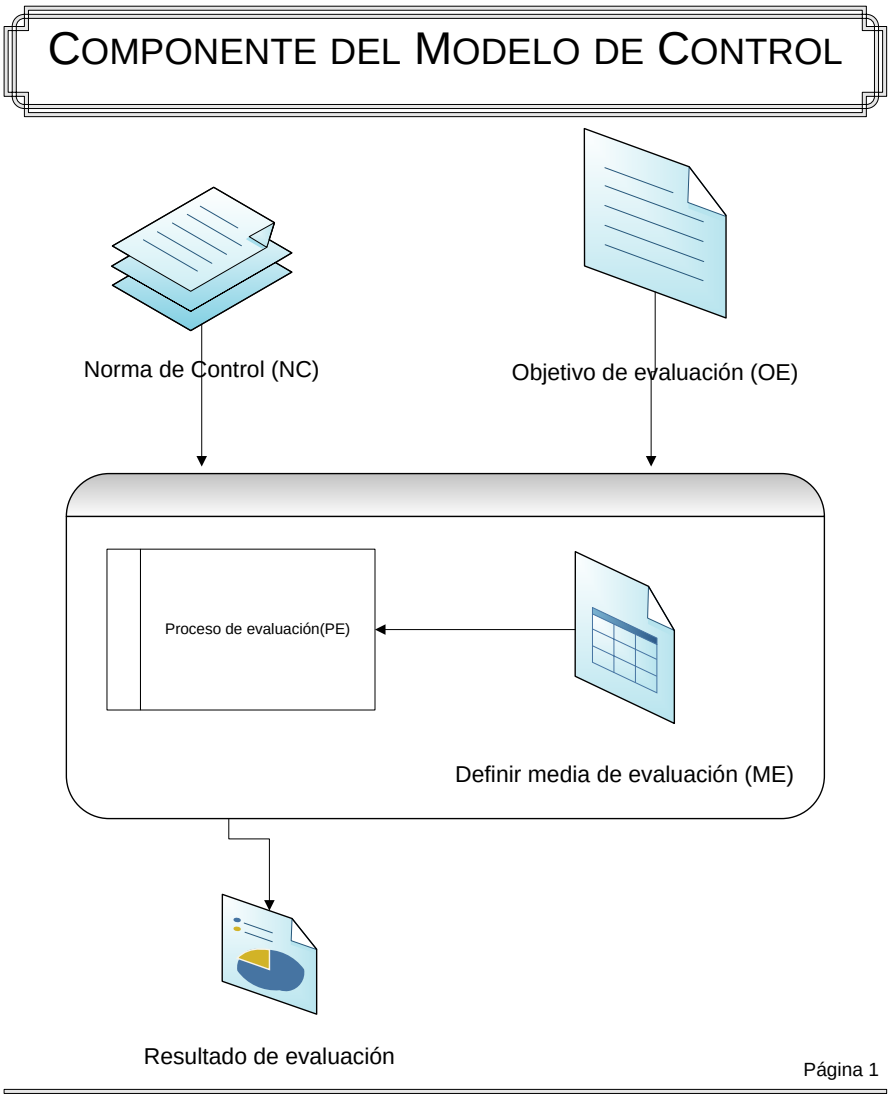

Figura 61, Componentes del Modelo de Control

Roles de responsabilidad

El modelo incluye los siguientes roles de responsabilidad:

Tabla 49

Roles de responsabilidad del modelo de control

Nombre	Rol
Responsable tecnológico de las entidades (RTE)	Responsable de las dependencias municipales a quien se aplicará el modelo y se evaluará.

Responsable del área de Control Tecnológico (RACT)	Responsable de evaluar de acuerdo a directrices identificadas por la norma

Fuente: López & Lala, 2013

Descripción de las actividades del modelo.

El diagrama de las actividades se presenta a continuación:

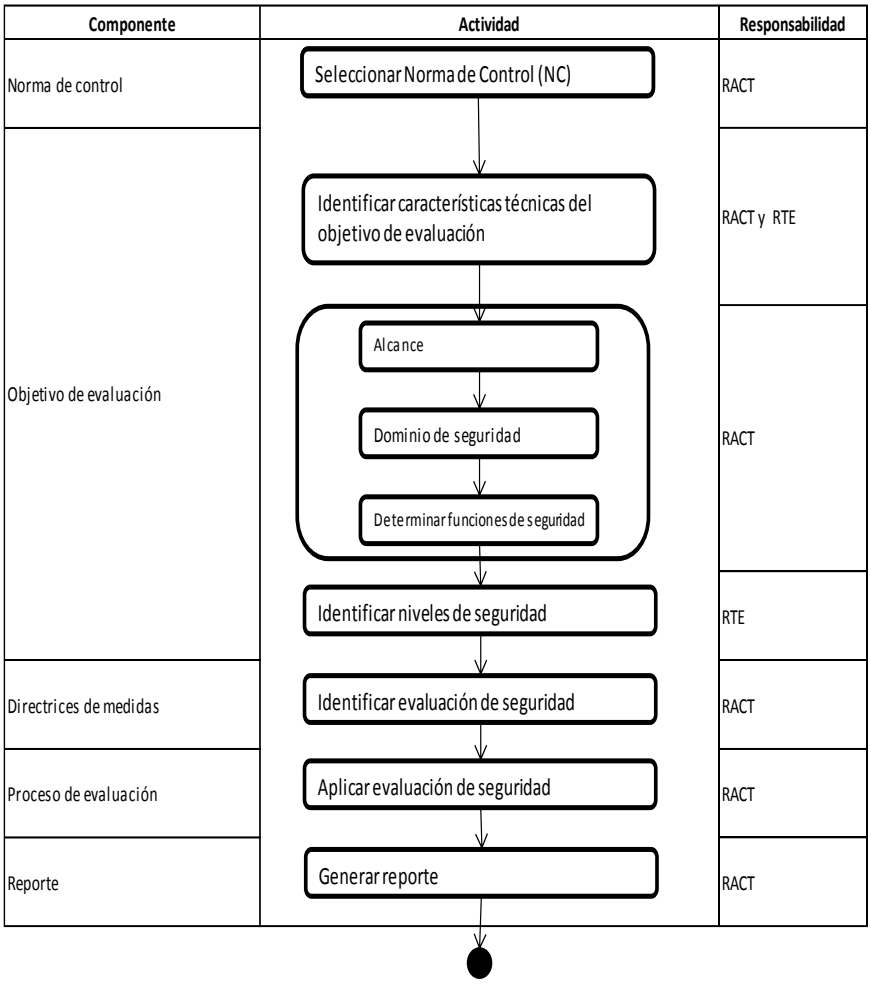

Figura 62, Descripción de las actividades del modelo

Seleccionar Norma de Control (NC).- Dependiendo de la necesidad a ser evaluada en la institución se toma la más apropiada para evaluar y monitorear los controles de tecnología. Este modelo de evaluación toma como apoyo los dominios de la ISO 27002:2009 (Tecnología de la Información – Técnicas de la Seguridad – Código de práctica para la gestión de la Seguridad de la Información).

El responsable de la actividad es el responsable del área de Control Tecnológico.

Identificar características técnicas del objetivo de evaluación.- Identificar los objetivos de evaluación, con los siguientes componentes:

- Alcance.- Representa al conjunto de dominios que van a ser utilizados para la evaluación.
- Dominio de seguridad.- representan a los dominios seleccionados para emplearlos como guía y de esta forma determinar la gestión adecuada para priorizar la gestión de riesgo.
- Determinar funciones de seguridad.- representa el nivel de riesgo que tiene la función de seguridad.
- Controles de seguridad.- son controles de seguridad actualmente implementados que se encuentran implementados en el dominio de seguridad.

Identificar niveles de seguridad.- Los niveles de seguridad de acuerdo a la Norma ISO 27002, son los descritos en el ítem "Punto de partida para la seguridad de la información".

De acuerdo a la experimentación existen el campo del impacto que está apoyado en los activos de información y el ítem de riesgo que representa al nivel de calificación del control del dominio con los siguientes valores "Incipiente"= 5, "Confiable"=3, "Optimo"=1.

Identificar Evaluación de Seguridad.- De acuerdo a los resultados obtenidos en la evaluación. La ponderación recomendada es la siguiente:

- Cumplimiento del control:
    - Seleccionar NO, indica que el control no se cumple se representa con el valor de 0
    - Seleccionar SI, indica que el control existe y se está cumpliendo, se representa con el valor de 1.

Una vez que se completado la evaluación, se puede determinar el nivel de cumplimiento, en base al criterio que se muestra en la siguiente tabla:

Tabla 50

Rango del cumplimiento para el modelo

Cumplimiento	Rango	Descripción de Cumplimiento
Cumplimiento Crítico	81 -100%	Los controles de seguridad no están completamente implementados junto con el entorno.
Cumplimiento regular	71 -80%	Existen ciertos controles definidos y no implementados.
Cumplimiento aceptable	41 - 60%	Existe un control de seguridad y más de la mitad de los controles implementados y ejecutados.
Cumplimiento adecuado	21 -40%	Existen controles definidos apoyados pero no implementados correctamente.
Cumplimiento ideal	0 -20%	Los controles de seguridad están definidos completamente, junto con la implementación del control.

Fuente: López & Lala, 2013

Aplicar evaluación de seguridad.

Se aplica la evaluación a cada dominio identificando los objetivos de control del dominio obteniendo como resultado el riesgo por dominio, por lo tanto, de acuerdo a la sumatoria de los valores en los dominios se puede determinar el nivel de riesgo por dominio, el nivel del riesgo está en base al criterio que se muestra en la siguiente tabla:

Tabla 51

Cuadro que representa a la determinación del nivel de riesgo

Nivel de riesgo	Nivel de riesgo
Alto	81 -100%
Medio Alto	71 -80%
Medio	41 - 60%
Medio Bajo	21 -40%
Bajo	0 -20%

Fuente: López & Lala, 2013

Generar el reporte

De acuerdo a los resultados obtenidos, se genera un reporte con el resultado general, donde se identifica los objetivos de control que deben bajar el riesgo y que deben ser evaluados constantemente.

4.2 Metodología de la Implementación del Modelo

La metodología propuesta para ejecutar la implementación del modelo es la siguiente:

- Diagnóstico del cumplimiento de las políticas.
- Simulación de controles
- Determinación de controles.
- Plan de acción.

Diagnóstico del cumplimiento de las políticas.- Corresponde a la evaluación del cumplimiento de los controles existentes en las áreas de la DMI y dependencias municipales; de ésta forma valorar los potenciales riesgos que amenazan a las áreas que conforman a la Dirección Metropolitana de Informática, utilizando el acuerdo N° 156, emitido por la Subsecretaria de Administración Pública referente al Esquema Gubernamental de la Seguridad de la Información la cual está fundamentada en las normas ISO 27002.

Esto se logra por medio de un diagnóstico que se puede realizar por medio de la contestación de un test, al cual se ha denominado "test de cumplimiento de políticas", este permite presentar controles vulnerables y sirve como punto de inicio a la institución para realizar una constante gestión en la revisión de controles.

Simulación de controles.- Una vez analizado la información se aplica el modelo de control para identificar el comportamiento de los dominios vulnerables como se detalla en el ítem "4.1.4".

Plan de acción.- En base al reporte de la evaluación obtenido se genera el plan de acción que determina las actividades a realizarse que van a permitir evaluar y monitorear en un tiempo determinado, ésta actividad se realizará con el Documento "plan de acción".

La hipótesis planteada en el capítulo I que establece "***Disminuir los niveles de riesgo de los controles en la mayoría de los casos tecnológicos establecidos por la***

DMI en el MDMQ, a través de un modelo de Evaluación y monitoreo del cumplimiento de controles de gestión Tecnológica adaptado a la realidad municipal"

De acuerdo a la hipótesis planteada en este estudio se pudo determinar con las experimentaciones un modelo que reduce el riesgo total de 62,38% (medio alto) al 18% (bajo) utilizando e implementando los controles que se menciona en la norma ISO 27002 (Tecnología de la Información – Técnicas de la Seguridad – Código de práctica para la gestión de la Seguridad de la Información).

El modelo va a permitir determinar cuáles son los dominios en los que la institución presenta riesgo de tal forma que al implementar los controles disminuya en gran porcentaje el riesgo y a través de la metodología de uso del modelo se pueda monitorear el cumplimiento de los controles en la institución municipal.

CONCLUSIONES

Una vez culminado este trabajo, se llegaron a las siguientes conclusiones:

- La literatura relacionada con la corriente del pensamiento de la seguridad de la información, es amplia y variada, se analizaron paper, libros, normas permitiendo analizar la normativa vigente que mantiene la institución utilizándose la norma Internacional ISO 27002 a través de la cual se evaluó la eficacia de los controles existentes en la gestión tecnológica de la Dirección Metropolitana de Informática.
- El levantamiento de información que se realizó a las dependencias desconcentradas que conforman la entidad municipal a través de encuestas, permitió obtener como resultado un análisis de riesgo a través del cual se identificó las amenazas, debilidades que presenta las áreas de tecnología, se obtuvo como riesgo total el 60,44% equivalente a un riesgo medio alto, los niveles de madurez alcanzados sobre los 130 controles aplicables se consolidaron en los dominios de la ISO 27002 obteniendo como resultado un nivel de madurez por dominio.
- Actualmente la Dirección Metropolitana de Informática no posee un modelo de evaluación y monitoreo de la gestión tecnológica que permita determinar el nivel de riesgo de la institución.
- La validación del modelo del presente trabajo de tesis, se realizó a través de 33 experimentos agrupados por dominio, utilizando valores de exposición que permitieron disminuir el riesgo total al 18% equivalente a riesgo bajo.
- El modelo de evaluación y monitoreo propuesto, permitirá al Distrito Metropolitano del Municipio de Quito – Dirección de Informática:
  - Determinar el riesgo total de tecnología que mantiene la institución.
  - Determinar los objetivos de evaluación que presentan un alto riesgo.
  - Identificar la eficacia de los controles en las dependencias desconcentradas de la municipalidad.

El modelo de Evaluación y Monitoreo propuesto va a permitir identificar los controles, procesos que tiene la institución y los que requieren mayor atención para

mejorar la eficacia y disminuir el riesgo, acompañado con jornadas de monitoreo en el cumplimiento de las políticas que va a permitir una mejora continua en el modelo. Actualmente la Dirección Metropolitana de Informática dentro de su modelo de gestión aplicado no presenta el área de Seguridad que apoye los objetivos tecnológicos.

Por último se concluye que el problema que la institución municipal presenta con un alto riesgo tecnológico, no se soluciona completamente con la implementación de procedimientos, normas o modelos, debido a que la decisión del usuario que opera es el que define en gran medida si ejecuta o no el control. Sin embargo todo queda en la decisión de la alta directiva que apruebe en invertir en recurso humano, tecnológico, capacitación los mismos que van a apoyar en la ejecución de actividades de evaluación y monitoreo tecnológico.

RECOMENDACIONES

Se recomienda la socialización y correcta aplicación de las Políticas de Gestión Tecnológica al personal de la institución con el objetivo de llevar un control en la Dirección Metropolitana de Informática.

De acuerdo al estudio realizado se recomienda disminuir el riesgo total, mediante la aplicación del Acuerdo N° 166, utilizando normas técnicas Ecuatorianas NTE INEN- ISO/IEC 27000 para la gestión de la Seguridad de la Información, en la Dirección Metropolitana de Informática y las Dependencias Municipales.

Se recomienda la aplicación del modelo del presente trabajo de tesis en la Dirección Metropolitana de Informática y las Dependencias Municipales, para disminuir el riesgo en la gestión tecnológica.

Se recomienda realizar evaluaciones en periodos de tiempo a las dependencias municipales para identificar el cumplimiento de los controles e identificar amenazas y vulnerabilidades que afectarían al core de negocio de la institución.

Se recomienda la aplicación de un modelo, que permita evaluar y monitorear el cumplimiento de los controles de la gestión tecnológica.

Se recomienda aplicar el modelo de Evaluación y Monitoreo propuesto, que permitirá identificar los controles, procesos que tiene la institución y los que requieren mayor atención para mejorar la eficacia y disminuir el riesgo, acompañado con jornadas de monitoreo en el cumplimiento de las políticas que va a permitir una mejora continua en el modelo.

Se recomienda crear el área de coordinación de la Seguridad Informática, en el cual se involucren todos los jefes de área en la administración de la seguridad para que ejecuten el modelo propuesto a través de la metodología de uso.

Concientizar a los funcionarios municipales que la responsabilidad de la seguridad de la información es responsabilidad de todos, con el apoyo directivo implementar un proyecto de capacitación a los servidores municipales.

BIBLIOGRAFÍA

27005:2012, N. I.-I. (2012). TECNOLOGIA DE INFORMACIÓN- TECNICAS DE SEGURIDAD- GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.

APM_Group. (2007). http://www. itil-officialsite.com/. (ITIL, Productor)

Bautista, L. A. (2013). Alcance del proyecto. En L. A. Bautista, Plan de Seguridad (págs. pag 7-8).

Bautista, L. A. (2013). Plan de Seguridad de la Información Compañia XYZ Soluciones.

Bejarano Ramos , C., Galarza Chiriboga , A., Rivera Moncayo , C., Ceballos , J., & Moncayo, M. (s.f.). Investigación para la elaboración del guión para documentales .

Calafat, A. L. (s.f.). Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros.

Calmaestra, L. B. (2005). Obtenido de Descartes 2D: recursostic.educacion.es/descartes/web/materiales_didacticos/unidimensional_lbarrios/definicion_est.htm

Carolina Benavides, A. H. (2011). Aplicaci´on de la norma COBIT en el monitoreo de transferencias. (V. 5. 1, Ed.) Publicaciones en Ciencias y Tecnolog´ıa.

COBIT, 4. (2007).

COBIT, 4. (2007). CRITERIOS DE INFORMACIÒN DE COBIT.

COSO. (2004). COMMITTEE OF SPONSORING ORGANIZATIONS.

COSO. (2009).

DeLaFuente. (2000). (E. c. TI, Editor) Obtenido de http://www.isaca.org.uy/

Dirección General para el Impulso de Electrónica. (2011). http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.UxaR9_ZqaYU, Magerit V3.

E. C. (2000). (2. Edicion, Ed.) Bogota, Colombia: Lito Perla Impresoras Ltda. 2000.

Estevez, J., & Estevez, G. (17 de 02 de 2003). Estadística Descriptiva. Obtenido de http://dieumsnh.qfb.umich.mx/estadistica/

Estructura conceptual integrada. (2000). (2, Ed.) Bogota, Colombia: Lito Perla Impresoras Ltda.

Gorgas, J., Cardiel, N., & Zamorano, J. (2009). ESTADÍSTICA BÁSICA. Madrid.

INEN ISO / IEC 27005. (2012).

ISACA. (2011). Information Systems Audit and Control Association. (C. f. control., Productor) Obtenido de http://www.isaca. org/knowledge-center/cobit/pages/ overview.aspx : www.isaca.org

Juan, Á. A., Fuente, B., & Vila, A. (2011). Estadística. Barcelona: Primera edición.

López, L., & Lala, J. (2013).

MAGERIT 1. (2012). MAGERIT 1 - Metodología de Análisis y Gestión.

Publican enfoque integrado de COBIT, I. e.-D. (2005). 2514-publican-enfoque-integrado-de-cobit-itil-e-iso-17799. Obtenido de http://www.datamation.com.ar: http://www.datamation.com.ar/noticias/311-varios/2514-publican-enfoque-integrado-de-cobit-itil-e-iso-17799

Rodríguez, V. K. (2010). Tesis de Auditoría Informática - SUPERTEL.

Tecnológico de Monterrey. (s.f.). Curso básico de Estadística. Obtenido de http://www.cca.org.mx/cca/cursos/estadistica/

Triola, M. (2009). LIBRO DE ESTADÍSTICA. México.

Vitutor. (2012). Definición de Estadística. Obtenido de http://www.vitutor.com/estadistica/descriptiva/a_1.html

ANEXOS