UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

UNIVERSIDAD DE FUERZAS ARMADAS ESPE

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

MAESTRÍA DE EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

SEGUNDA PROMOCIÓN

EVALUACIÓN TÉCNICA DE SEGURIDADES DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LAS NORMAS ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005.

Tesis De Grado

Autores: Ing. Diego Santiago Aguirre Freire

Ing. Jhon Carlos Palacios Cruz

SANGOLQUI, MARZO 2014

Dirección Metropolitana de Informática

Administración General

Quito, 19 de febrero de 2013

CARTA DE AUSPICIO

DIRECCIÓN METROPOLITANA DE INFORMÁTICA, AUSPICIA la Tesis de Grado para Obtener el Título de Máster en Evaluación y Auditoría de Sistemas Tecnológicos en la Escuela Politécnica del Ejercito, denominada "EVALUACIÓN TÉCNICA INFORMÁTICA DE LA SEGURIDAD DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LAS ISO 27001 Y 20072", Que será realizado por Sr. Ing. Diego Santiago Aguirre y Sr. Ing Jhon Carlos palacios Cruz.

Ing. Jefferson Capelo

DIRECTOR METROPOLITANO DE INFORMÁTICA

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO DE TUTORÍA

Ing(a). Magali Reascos M.S. C.

CERTIFICO:

Que el trabajo titulado "EVALUACIÓN TÉCNICA DE SEGURIDADES DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LASNORMAS ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005.", realizado por Diego Santiago Aguirre Freire y Jhon Carlos Palacios Cruz, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

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

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

Sangolquí, Marzo de 2014

_____

Ing(a). Magali Reascos M.S. C.

DIRECTOR DE PROYECTO

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Diego Santiago Aguirre Freire y Jhon Carlos Palacios Cruz

DECLARAMOS QUE:

El proyecto de Maestría denominado "EVALUACIÓN TÉCNICA DE SEGURIDADES DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LAS NORMAS ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005.", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el trabajo correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

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

Sangolquí, Marzo de 2014

Ing. Diego Santiago Aguirre Freire

Ing. Jhon Carlos Palacios Cruz

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Diego Santiago Aguirre Freire y Jhon Carlos Palacios Cruz

Autorizamos a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la Institución, del trabajo ""EVALUACIÓN TÉCNICA DE SEGURIDADES DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LAS NORMAS ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005.", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 12 de Marzo de 2014

Ing. Diego Santiago Aguirre Freire

Ing. Jhon Carlos Palacios Cruz

AGRADECIMIENTO

Agradezco a mis padres por su cariño, enseñanzas y sabiduría que me fomentaron, con los cuales han sido una herramienta valiosa en mi vida desde mi niñez.
Agradezco a las autoridades de la Dirección Metropolitana de Informática y a su Director Ing. Jefferson Capelo el cual permitió desarrollar nuestro tema de la tesis con el cual damos cumplimiento a una etapa más de nuestra educación.
A Carlos Sani Jefe del área del Infraestructura tecnológica por brindar me la información necesaria para el cumplimiento de la tesis.

Ing. Diego Santiago Aguirre Freire

AGRADECIMIENTO

A Dios que me permitió hacer realidad un sueño, brindándome fortaleza perseverancia para llevar a cabo mi meta.

A la ingeniera Magali Reascos, Tutora de Tesis y al Ingeniero Mario Ron, Coordinador de Tesis, quienes aportaron con sus consejos y conocimientos a la construcción de esta meta.

A mi compañero de Tesis Ingeniero Santiago Aguirre, por su colaboración y apoyo incondicional en todos los difíciles momentos en el desarrollo de nuestra tesis.

A todos quienes de una u otra manera nos han ayudado sin ningún interés al desarrollo de este proyecto.

A todos ellos, muchas gracias.

Ing. Jhon Carlos Palacios Cruz

DEDICATORIA

A mis padres ya que son el motor de mi vida, por su amor, apoyo, educación con los cuales me ha vuelto, un ser de bien.
A mí enamorada por su apoyo y comprensión los cuales me a brindo en este tiempo que la he conocido.
A mis hermanos los cuales los quiero mucho, y final mente a mis queridos sobrinos los cuales con su alegría me brindan energía.

Ing. Diego Santiago Aguirre Freire

DEDICATORIA

Me gustaría dedicar esta Tesis a Dios y a mi Familia.

A mi madre Imelda Cruz y en especial a mi padre Raúl Palacios que aunque no estando presente físicamente sé que siempre estuvo ahí, en mi mente y corazón a mi madre por su amor, ánimo y su cariño teniendo muy en claro los principios de respeto y responsabilidad y sabiendo que todo lo que soy es gracias a ella.

A mis hermanos Elizabeth, Danilo, Guillermo y mis sobrinos Cristian, Anthony, Stefanía, por su afecto, cariño y bondad.

Esto y mucho más para ustedes.

Ing. Jhon Carlos Palacios Cruz

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El MDMQ maneja información sensible de la ciudadanía, como lo es la información catastral, licencia metropolitana única para el ejercicio de actividades económicas, pagos de impuestos prediales, declaración de patente y 1,5 x 1000 en activos, regularización de edificaciones existentes entre otras. Dicha información es crítica la cual se encuentra alojada en los servidores y sistemas de almacenamiento ubicados en el Data Center, por lo que es necesario que se garantice su confidencialidad, integridad y disponibilidad. El presente trabajo se orienta a la evaluación técnica informática para determinar el cumplimiento de las normas y estándares internacionales que establecen un GAP de la gestión de seguridad de la información, según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005. Cabe señalar que dicho trabajo, se desarrollará mediante una investigación documental - descriptiva, para la recolección de la información se empleará técnicas de investigación de campo de fuentes primarias, como son la observancia y la entrevista; y secundarias como son documentos y libros dicha información, será analizada y evaluada, mediante lo cual, se determinará el cumplimiento o no de los lineamientos según la norma ISO/IEC 27002:2005, con el fin de identificar vulnerabilidades de seguridad en el de todos los elementos que se encuentran en Data Center y recomendar se establezcan políticas de seguridad de la información y se implemente controles para el manejo de riesgos, monitoreo y revisión del desempeño y efectividad del Data Center, considerando el mejoramiento continuo de la seguridad.

PALABRAS CLAVE

Disponibilidad.

Confidencialidad.

Trazabilidad.

Autenticidad.

Hallazgo.

ABSTRACT

The MDMQ handles sensitive information from the public, such as cadastral information, only metropolitan license to practice economic activities, property tax payments, patent statement and 1.5 x 1000 in assets, regularization of existing buildings among others. Such information is critical that it is hosted on servers and storage systems located in the data center, so it is necessary that its confidentiality, integrity and availability is guaranteed. This paper is oriented to computer technical evaluation to determine compliance with international norms and standards that establish a GAP management information security according to ISO / IEC 27001:2005 ISMS and ISO / IEC 27002:2005 standards. It should be noted that this work will be developed through documentary research - descriptive , for the collection of information from field research techniques will be used primary sources , such as enforcement and interview, and secondary documents such as books and such information will be analyzed and evaluated , whereby the fulfillment or not of the guidelines will be determined according to ISO / IEC 27002:2005 standard, in order to identify security vulnerabilities in all the elements found in Data Center and recommend policy information security controls are established and risk management , monitoring and review of performance and effectiveness of the data Center is implemented, considering the continuous improvement of safety.

Key Words

Active

Availability

Confidentiality

Traceability

Authenticity

CAPÍTULO I

EVALUACIÓN TÉCNICA DE SEGURIDADES DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LASNORMAS ISO/IEC 27001:2005 SGSI E ISO/IEC 27002:2005.

Es de conocimiento público que hoy en día la informática se ha convertido en uno de los pilares principales de las organizaciones ya que la base del negocio es manejada o se encuentra en una plataforma informática, lo cual es de gran importancia y hasta en muchos casos depende de está la continuidad del negocio, ya que se lleva a cabo transacciones comerciales, comunicaciones o servicios, por todos estos puntos es vital contar con una evaluación de sistemas , procesos, políticas y contar con una idea de cuáles son los riesgos y que tipo de impactos tendrían si se interrumpiera su normal funcionamiento.

La principal inquietud de la Dirección Metropolitana de Informática (DMI)está enfocado en el Data Center que es el núcleo donde se encuentra alojada la información y las diferentes aplicaciones o sistemas que son muy importantes para el normal desempeño del MDMQ.

Por este motivo se realiza una evaluación técnica de seguridades del Data Center con el objetivo de valorar y determinar el grado de cumplimiento de los controles de la norma ISO/IEC 27002:2005de los procesos críticos del negocio que se encuentran alojados en el Data Center, teniendo como marco de referencia la ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.

El proceso de la evaluación se realizó con una metodología basada en riesgos la cual permite generar resultados confiables y si fuese el caso tomar medidas preventivas o correctivas por parte de las autoridades de la DMI.

1.1 Justificación e Importancia

El Data Center del Municipio tiene en su visión cumplir con el crecimiento ordenado de toda su infraestructura tecnológica, seguridad física, uso de energía eficiente y confiable, respaldo de información crítica y sensible, adaptabilidad al avance tecnológico, todo esto en condiciones de humedad y temperatura de acuerdo con las recomendaciones de los fabricantes de los equipos para garantizar el buen funcionamiento del equipamiento, uso y conectividad en cuanto a integración de diferentes plataformas y dependencias del MDMQ.

El Data Center del MDMQ aloja varias tecnologías, que brindan servicios de suma importancia a sus clientes externos (ciudadanía de Quito) como también a los clientes internos (usuarios de las dependencias Municipales y Empresas Municipales). Estos servicios son críticos y de vital importancia.

El MDMQ en la actualidad ha integrado sus sistemas tecnológicos con los servicios de la banca, cooperativas y empresas de tarjetas de crédito para facilitar a la ciudadanía el pago de sus obligaciones en cualquier momento y en cualquier lugar. Esta articulación obliga al MDMQ a mantener una calidad de servicio los 356 días del año.

El MDMQ se beneficiará con este proyecto, pues al realizar la evaluación técnica del Data Center y presentar el documento final con los hallazgos, se podrán aplicar correctivos y a su vez establecer políticas, procesos y controles de seguridad.

1.2 Planteamiento del problema

El MDMQ no cuenta con un plan formal de continuidad del negocio, lo cual conlleva a que en caso de sufrir un incidente grave, de tipo ambiental, terrorista y/o político, no sería posible restablecer sus operaciones en un tiempo prudencial.

El manejo de procedimientos de seguridad del Data Center del MDMQ no se encuentra debidamente documentado, y procede bajo lineamientos informales, lo cual representa un riesgo y podría causar fuga de información o un incidente fortuito, lo cual afectaría el normal funcionamiento de los servicios de TI, que se encuentran implementados en los servidores e infraestructura del Data Center.

En el MDMQ, se desarrollan los sistemas, según una metodología que completa el ciclo de vida, diseño, análisis, construcción, pruebas e implementación, lo cual se desarrolla en ambientes estrictamente definidos como son un ambiente de desarrollo, pruebas y producción, en cada una de estas etapas, se procede a documentar. Pero existen sistemas que por orden de la gerencia se los debe dar prioridad de forma que estos no cumplen con el proceso antes mencionados lo cual es un verdadero problema ya que al no contar con las diferentes validaciones y la documentación respectiva, se puede tener fallas en su funcionamiento en el ambiente de producción.

Los controles de accesos a las cuentas de tipo administrativas para el ingreso a los sistemas, servicios, equipos de procesamiento de información son manejadas por varias personas, no existe una política de control de acceso a usuarios privilegiados, cabe señalar que es necesario que exista un registro de los accesos y monitoreo continuo de los mismo.

Al presentarse un incidente de seguridad, éste no es debidamente documentado, por lo que al tener una reincidencia, no se puede solucionar de una forma oportuna, ya que no existe un registro, en el cual conste el procedimiento para resolver dicho incidente, y se tendría que volver a analizar y buscar la posible solución.

1.3 Formulación del problema

- ¿Identificar si los procedimientos documentados actuales que posee el MDMQ se cumplen y están bajo los lineamientos y normas de seguridad internacionales ISO/IEC 27002:2005?
- ¿Determinar qué tipo de problemas puede conllevar el acceso a las instalaciones de personas no autorizadas en el data center?
- ¿Cuál es el impacto de colocar en una ambiente de producción un sistema que no haya cumplido con todo el ciclo de vida correspondiente?
- ¿Identificar si se cumple con el registro en bitácoras de los cambios y configuraciones que se realizan a los sistemas, programas, equipos y de incidentes, errores y problemas que se presentan?

1.4 Objetivo General

Aplicar una evaluación técnica informática al Data Center del MDMQ, utilizando matrices de impacto y probabilidad además de validar el grado cumplimiento de la norma ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005, para que en base a los hallazgos encontrados se presente en un informe a las autoridades y estas puedan tomar medidas preventivas o correctivas.

1.5 Objetivos Específicos

Los objetivos específicos son los siguientes:

- Investigar las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005
- Establecer el nivel de cumplimiento de acuerdo a los lineamientos de las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.
- Evaluar los procedimientos de seguridad actuales que posee el Data Center tienen según el como marco de referencia la ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.
- Elaborar el informe final de la evaluación técnica donde se plasmarán los hallazgos, observaciones y recomendaciones.

CAPÍTULO II

2.1 Marco Teórico

2.1.1 Antecedentes del estado del arte

Empresas establecidas en el Ecuador se han certificado con la normas ISO/IEC 27001:2005 SGSI.La primera fue TELCONET empresa de provisión de servicios de comunicación de video, voz y datos en el año 2008. TELCONET mantiene certificaciones a nivel empresarial ISO/IEC 27001:2005 SGSI en Sistemas de Seguridad de la Información además a nivel de recursos humanos (Maestría en Ciencias Redes de Información, CCNA, CCDA, CCNP, CCDP, CCIE, CSE CFFX, CWNA, etc.).(Quezada, 2012)

Otra empresa es el caso de Telefónica Movistar Ecuador, empresa que en febrero de 2011 recibió la certificación del "Sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001:2005SGSI", otorgado por la Asociación Española de Normalización y Certificación (AENOR). Esta certificación "tiene relación con la provisión y soporte del servicio de datos fijos e internet dedicado para el segmento de grandes empresas" (...), (Movistar, 2011)

En la Cuidad de Quito en el 2011 se ha establecido la Empresa Pública Metropolitana De Agua Potable y Saneamiento, Miguel Ángel Játiva (2011) afirma: "en el plan estratégico se han establecido normas de seguridad de Información ITIL e ISO 27001" (Játiva, 2011, p.44)

Para solventar inconvenientes al no existir una coordinación adecuada entre las áreas usuarias con el Departamento de Tecnología Informática, respecto a la rotación del talento humano de la Empresa y el no disponer de una herramienta que permita normar el uso de accesos a los servicios y sistemas informáticos, ha

originado, que el personal de Tecnología Informática no proceda a la desactivación de los usuarios claves, y a su vez no se cuente en esta área con un registro actualizado de los mismos en la Empresa. (Játiva, 2011, p.44)

Otro ejemplo de adopción de esta norma ISO, es el Banco Central de República Dominicana que en el año 2011.

> El Banco Central de República Dominicana se convirtió en el primer banco de su tipo en América Latina en adquirir la certificación ISO 27001, informó el gobernador Héctor Valdez Albizu, durante un acto al que asistieron todos los funcionarios y empleados de la institución.
>
> La certificación fue emitida por la empresa noruega DetNorske Veritas S.A., luego de realizar la auditoría final que acredita que el proceso de Certificados de Inversión del Banco Central cumple con todos los requisitos de seguridad de la información establecidos bajo la Norma ISO/IEC 27001:2005 SGSI(…). (Crónica Central, 2012)

2.1.2Marco Teórico

2.1.2.1 Seguridad de la información

Uno de los principales activos más valioso para las organizaciones es su información, la cual está amenazada por diferentes factores ya sean internos o externos a las organizaciones. La implantación de los sistemas de información, como la aparición de las nuevas tecnologías ha aumentado los riesgos de robo, alteración, pérdida de la información, por tal motivo las organizaciones deben adoptar políticas de seguridad en todos sus procesos del negocio y sobre todo los tecnológicos. (ISO/IEC 27001:2005, pág. 10)

2.1.2.2 Eventos de seguridad de la información

Es un evento inesperado ya sea de un sistema o de servicio de red, que define una posible violación o interrupción y afecta directamente a las políticas de seguridad de la información de gran impacto a la empresa.(ISO/IEC 27001:2005, pág. 10)

2.1.2.3 Incidente de seguridad de la información

Son sucesos no programados de carácter de seguridad que comprometen el buen funcionamiento de las operaciones de la empresa y amenazan la seguridad de la información.

Estos tipos de imprevistos deben ser evitados y en lo posible mitigados, para lo cual se deben tomar muchas acciones con el fin de salvaguardar la información y deben ser registrados, en una bitácora en la cual se encuentre detallado el problema y como fue superado.(ISO/IEC 27001:2005, pág. 10)

2.1.2.4 Integridad

Es garantizar que la información no sea alterada por accesos no autorizados, tanto en su procesamiento como en su almacenamiento, además el de poder identificar cualquier alteración maliciosa que se pudiera presentar.(ISO/IEC 27001:2005, pág. 10)

2.1.2.5 Riego Residual

Es el riego resultante después de haber aplicado las medidas de seguridad contra el riesgo. (ISO/IEC 27001:2005, pág. 11)

2.1.2.5.1 Aceptación del Riesgo

Esto se procede cuando en el análisis de riesgo no tiene tanto impacto e importancia. (ISO/IEC 27001:2005, pág. 11)

2.1.2.5.2 Análisis de Riesgo

Consta de varios procedimientos con el fin de identificar los riesgos más importantes y su fuente, para tener una proyección del daño que puede causar a los sistemas o a la seguridad de la información.(ISO/IEC 27001:2005, pág. 11)

2.1.2.5.3 Evaluación del Riesgo

2.1.2.5.3.1 General

Análisis y estudios de la importancia de cada uno de los riesgos y las consecuencias que estos traerían sino se realiza ningún proceso para mitigarlo. (ISO/IEC 27001:2005, pág. 11)

2.1.2.5.3.2 Gestión de Riesgo

Procedimientos y actividades que se realizan para mitigar el riesgo.(ISO/IEC 27001:2005, pág. 11)

2.1.2.5.3.3 Tratamiento del Riesgo

Procedimiento para la toma de medidas y posterior implementación para tratar el riesgo.(ISO/IEC 27001:2005, pág. 11)

2.1.2.5.4 Enunciado de Aplicabilidad

Registro documentado donde se detallan los controles más importantes implantados en el modelo SGSI de la institución.(ISO/IEC 27001:2005, pág. 11)

2.1.3 Normas ISO/IEC

2.1.3.1Norma ISO/IEC 27001:2005

La norma ISO/IEC 27001:2005 SGSI fue diseñada por el Comité Técnico de la Organización Internacional para la Estandarización y sus siglas son ISO el 15 de Octubre del 2005 este Estándar Internacional ha sido concebido con el afán de definir, desarrollar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI).

El objetivo de adoptar esta norma es desarrollar e implementar el SGSI de una empresa, para permitirle gestionar la seguridad de la información.(ISO/IEC 27001:2005, pág. 5)

La norma ISO/IEC 27001:2005 SGSI define como una organización limita, desarrolla, e implanta un SGSI basado en el modelo PDCA y este comprende el Anexo A donde están descritos los controles de seguridad de la información, fundamentales que son importantes para reducir y minimizar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información.

Esta norma propone un modelo PDCA que está compuesto de cuatro pasos que son: Planear – Hacer – Chequear – Actuar, aplicado a los procesos del SGSI, ya que es un modelo de mejoramiento continuo.(ISO/IEC 27001:2005, pág. 6)

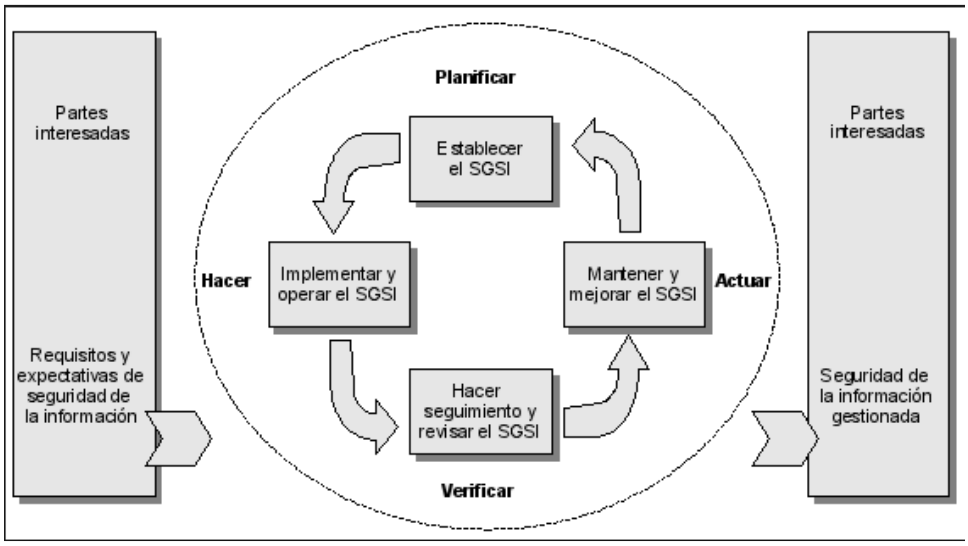

Figura 1 Modelo PDCA aplicada a los procesos SGSI (ISO 27001:2005)

2.1.3.1.1 Planear

Es crear políticas, objetivos, procesos y procedimientos del SGSI, los cuales permiten optimizar el manejo del riesgo y obtener una idea macro del mejoramiento de la seguridad de la información, cabe señalar que dichas políticas deberán estar alineadas con las políticas internas de la empresa u organización.(ISO/IEC 27001:2005, pág. 7)

2.1.3.1.2 Hacer

Ejecutar las políticas, objetivos, procesos y procedimientos que se encuentran en el SGSI.(ISO/IEC 27001:2005, pág. 7)

2.1.3.1.3 Chequear

Hacer un levantamiento de información y verificar si se ha cumplido con los objetivos establecidos en el SGSI, lo cual generará un informe donde se encuentren plasmados los resultados y novedades encontradas.(ISO/IEC 27001:2005, pág. 7)

2.1.3.1.4 Actuar

Definir decisiones para la corrección de los hallazgos encontrados y sin descartar acciones preventivas.(ISO/IEC 27001:2005, pág. 7)

Este modelo PDCA fue concebido con el fin de aplicar a todo tipo de empresa u organización, sin importar si es empresa pública o privada, ya que aplicando este modelo de manera correcta se podrá manejar de forma efectiva el riesgo del sistema de información, así se podrá mitigarlo, aceptar o evitarlo.

2.1.3.2 Sistema de gestión de seguridad de la información

2.1.3.2.1 Generalidades

Tiene como base fundamental el riesgo de negocio para lo cual debe proceder a nivel gerencial con el diseño de diferentes actividades para el mejoramiento de la seguridad de la información.

La empresa debe establecer continuamente el mejoramiento del SGSI con el modelo PDCA y su debida documentación, estas deben estar registradas en un documento donde se encontrara todas las actividades y operaciones que se realicen, también deben estar contempladas en un plan de actividades utilizando el mismo modelo. (ISO/IEC 27001:2005, pág. 12)

2.1.3.2.2 Establecer y manejar el SGSI

2.1.3.2.2.1. Establecer el SGSI

La organización debe delimitar el alcance y los límites del SGSI, bajo los términos del negocio, políticas de la organización y definir procedimiento para la identificación, evaluación y posterior mitigación del riesgo, teniendo en cuenta

siempre el impacto que el riesgo puede ocasionar sino se posee un mecanismo efectivo de la implantación de controles.(ISO/IEC 27001:2005, pág. 12)

2.1.3.2.2.2 Implementar y operar el SGSI

La organización para implementar y operar el SGSI debe realizar los siguientes pasos:

- Poseer un plan de tratamiento del riesgo donde se encuentren establecidas las acciones por parte de la gerencia los recursos, el financiamiento, roles y responsabilidades.
- Definir el proceso de implantación para el plan de tratamiento del riesgo, con el cual se conseguirá los objetivos planteados.
- Implantación de los controles y posteriormente medir si con ellos se lograron conseguir los resultados requeridos.(ISO/IEC 27001:2005, pág. 15)

2.1.3.2.2.3 Monitorear y revisar el SGSI

Realizar procedimientos de monitoreo a los controles para conseguir identificar si existen o no errores y estos poderlos resolver a tiempo, ayudar a determinar los eventos de seguridad críticos detectados y concebir políticas que mitiguen de manera segura y efectiva estos riesgos. (ISO/IEC 27001:2005, pág. 15)

2.1.3.2.2.4 Mantener y mejorar el SGSI

Una vez revisada la implantación del SGSI se debe proceder con las mejoras al SGSI ejecutando las medidas correctivas y preventivas necesarias mejorando los

controles que carecen de efectividad y cambiarlos por otros los cuales ayuden a conseguir los objetivos deseados.

La organización tiene que:

- Implementar cualquier mejora identificada.
- Llevar a cabo acciones correctivas y preventivas apropiadas aplicando las lecciones aprendidas de la experiencia en seguridad de la propia organización y la de otras.
- Comunicar los resultados y las acciones y acordarlos entre todas las partes interesadas.
- Asegurar que las mejoras logren alcanzar los objetivos previstos. (ISO/IEC 27001:2005, pág. 16)

2.1.3.2.3 Requerimientos de documentación

2.1.3.2.3.1 General

Todas las actividades, decisiones, acciones y políticas creadas deben ser registradas para ser monitoreadas, para la evaluación de su efectividad.

El documento debe tener registrado lo siguiente:

- Declaración de la política y objetivos de control.
- El alcance del SGSI
- Los procedimientos y controles que dan soporte al SGSI
- Una descripción de la política de valoración de riesgo
- La valoración del informe de riesgo
- El plan de tratamiento de riesgos

- Los procedimientos documentados necesarios para que la organización se asegure la planificación efectiva
- Los registros requeridos por la norma
- La declaración de aplicabilidad (ISO/IEC 27001:2005, pág. 17)

2.1.3.2.3.2 Control de documentos

Los documentos que se manejan deben ser protegidos y controlados de las manipulaciones del mismo, con el fin de salvaguardar la integridad y se pueda tener la confianza de los registros a través del tiempo.(ISO/IEC 27001:2005, pág. 17)

2.1.3.2.3.3 Control de registros

Se debe tener los registro de visitantes, registros de auditoria y solicitudes de acceso legibles y en buen estados para poder tenerlos en caso de necesitarlos posteriormente.(ISO/IEC 27001:2005, pág. 17)

2.1.3.2.4 Responsabilidad de la gerencia

En esta etapa debe estar contemplada el compromiso por parte de la gerencia con el fin de apoyar a las políticas del SGSI donde tienen roles muy importantes para lograr los objetivos deseados dentro de la organización u organización. Con el fin de estar en capacidad de tomar decisiones para la adecuada aplicación de los controles.

Debe existir evidencia del compromiso que tiene la gerencia con la organización, el mismo que debe contemplar que se cumplan las políticas de SGSI y los objetivos planteados.

Es de vital importancia que se establezcan roles y responsabilidades, asegurando que las personas asignadas se encuentren capacitas y tengan el conocimiento suficiente, es necesario que los recursos sean suministrados de manera efectiva y sobretodo que el criterio de nivel de riesgos se encuentre dentro de los niveles aceptables dentro de la organización.

La gerencia debe monitorear que se ejecuten auditorías internas, para así controlar que se cumplan con los controles establecidos.

La gerencia al proporcionar los recursos de manera efectiva se asegura que exista un correcto desempeño del SGSI.

Las personas responsables de ejecutar el SGSI deben estar capacitadas y conocer ampliamente del tema, debe determinarse las competencias, evaluar si es necesario cursos de capacitación, para un correcto desempeño es indispensable evaluar la eficacia del personal, para tener un resultado óptimo en la implementación del SGSI es imprescindible que el equipo en conjunto con los directivos sean conscientes de la importancia de sus actividades. (ISO/IEC 27001:2005, pág. 18)

2.1.3.2.5 Auditoria interna SGSI

En todas las Instituciones se debe realizar auditorías internas al SGSI con determinada frecuencia porque con ello podemos definir si se cumplen las observaciones realizadas y se verifica el cumplimiento de los objetivos del SI establecidos por parte de la gerencia. (ISO/IEC 27001:2005, pág. 20)

2.1.3.2.6 Revisión gerencial del SGSI

El SGSI debe ser revisado por parte de la gerencia por lo menos una vez al año, para garantizar que exista continuidad y eficacia. El SGSI indica las mejoras continuas que deben realizarse, mencionando las políticas y objetivos de la seguridad de la información.

Es indispensable contar con la autorización por parte de la gerencia donde indican que los objetivos a conseguir, los mismos que deben estar encaminados para el beneficio de la organización.

Es muy importante que los resultados que arroje la auditoria sean tomadas muy en cuenta, ya que en ellas se encuentran plasmadas la situación exacta del SGSI de la organización y mediante estas se puedan tomar las respectivas medidas del caso. (ISO/IEC 27001:2005, pág. 20)

2.1.3.2.7 Mejoramiento del SGSI

2.1.3.2.7.1 Mejoramiento continúo

Una de las partes fundamentales y de gran responsabilidad que tiene la organización es el mejoramiento continuo, que lleva a la efectividad del SGSI, mediante la correcta implantación de políticas de seguridad de la información, evaluación de los resultados de auditoría, monitoreo y análisis constante de los eventos encontrados, los mismos que deben ser revisados y supervisados por la gerencia de la organización.

Cabe mencionar que el análisis de eventos monitorizados, es un punto de vital importancia, ya que nos presenta conceptos de control; tales como las métricas

e indicadores, estas métricas e indicadores ayudan a controlar cómo transcurren los controles de la organización en el día a día.

Para que exista un verdadero mejoramiento del SGSI, se deben modificar los procedimientos y aplicar los controles necesarios en los requerimientos y procesos del negocio, en los niveles de riesgo y también en los criterios de aceptación de riesgo que se maneja dentro de la organización.

Es importante mencionar que debe existir mejora de los métodos de medida de la eficacia de los controles en base a la necesidad de los recursos. (ISO/IEC 27001:2005, pág. 22)

2.1.3.2.7.2 Acción correctiva

La acción correctiva nos permite eliminar la causa de una no conformidad basándose en el requerimiento de SGSI y de esta manera minimizar la probabilidad de que estos vuelvan a ocurrir.

Se debe generar un procedimiento para registrar:

- Las no-conformidades detectadas.
- Determinar las causas de las no-conformidades.
- Evaluar la necesidad de las acciones a llevar a cabo
- Determinar la acción correctiva a implementar
- Llevar un registro correcto de las acciones tomadas.(ISO/IEC 27001:2005, pág. 22)

2.1.3.2.7.3 Acción preventiva

Las acciones preventivas nos permiten eliminar la causa raíz de las no conformidades potenciales. Las acciones preventivas a realizar deben estar de acuerdo al impacto de los potenciales problemas. Es necesario identificar las posibles causas de esa no conformidad potencial, analizar posibles acciones a ejecutar e implantarlas y realizar el correspondiente seguimiento, con la verificación y comprobación de la eficacia, todo ello debidamente registrado.

El procedimiento que registre una acción preventiva es similar al que se lleva con una acción correctiva.(ISO/IEC 27001:2005, pág. 22)

2.1.4 Norma ISO/IEC 27002:2005

La norma ISO/IEC 27002:2005 es un que describen objetivos de controles que deben ser aplicados para la seguridad de la información de una organización u organización. Esta norma consta de 39 objetivos de control y 133 controles, divididos en 11 dominios de seguridad.

La Norma ISO/IEC 27002:2005 no solo se referencia a las áreas de tecnología de la información si no también enfoca asuntos organizaciones, seguridades físicas, gestión de personal, administración de políticas, etc.

La norma ISO/IEC 27002:2005 es un documento referencial para la implementación no es una norma certificable.

Figura 2. Once Dominios de Seguridad ISO/IEC 27002:2005

Los dominios de la norma ISO/IEC 27002:2005 son:

2.1.4.1 Políticas de seguridad

La gerencia debe guiar para la creación, aprobación, cumplimiento y mantenimiento de políticas de seguridad de la información, estas deben enfocarse en los lineamientos de la organización. (aglone3, 2013)

2.1.4.2 Organización de la seguridad de la información

Se refiere a que la gerencia debe apoyar a la seguridad de la información en la organización tanto con recursos internos, como con recursos externos, para mantener las tendencias actuales de las organizaciones para evitar el fraude, robo, alteración de la información, etc.(aglone3, 2013)

La gerencia de las organizaciones deben apoyar de forma clara la seguridad de la información, asignando roles y responsabilidades a cada una de las personas. (aglone3, 2013)

2.1.4.3 Gestión de activos

En este punto se refiere a la adecuada protección de los recursos de las organizaciones, los cuales deben estar inventariados y deben poseer un responsable para su mantenimiento, además de la generación de directrices para la clasificación de la información.

Existen varios activos dentro de las organizaciones

- Información: Registros digitales, base de datos, manuales, bitácoras, registros, etc.
- Activos de Software: Aplicaciones, licencias, herramientas, etc.
- Activos físicos: Equipos de cómputos, dispositivos móviles, equipamiento de comunicación, etc.
- Servicios: aire acondicionado, iluminación, energía, etc.
- Personas, capacitaciones, experiencia.

(aglone3, 2013)

2.1.4.4 Seguridad de los recursos humanos

Se refiere a todos los controles que deben establecer para evitar el robo, fuga de información por parte de los empleados, contratistas y terceras personas, que laborar en las actividades de la organización. Antes, durante y posterior al ciclo de trabajo. (aglone3, 2013)

2.1.4.5 Seguridad física y del entorno

Se debe precautelar los activos de amenazas físicas y ambientales para evitar la interrupción de las actividades de la organización. Esto manteniendo los activos

de la organización en áreas seguras y con el equipamiento adecuado.(aglone3, 2013)

2.1.4.6 Gestión de comunicaciones y operaciones

Se refiere al correcto manejo, procesamiento, operación y monitoreo de la información de la organización, para evitar la negligencia por mal uso deliberado de está, por parte de todos los usuarios internos y externos.(aglone3, 2013)

2.1.4.7 Control de acceso

Cada usuario de la organización debe manejar únicamente la información con la que trabaja, y no tener acceso a toda la información de la organización. Además la organizaciones deben contar con políticas de no divulgación y autorización al acceso de la información.(aglone3, 2013)

2.1.4.8 Adquisición, desarrollo y mantenimiento de sistemas de información

En los sistemas de información constan de varios elementos como son de infraestructura, aplicaciones, servicios, elementos de comunicación entre otras. Todos estos sistemas de información deben cumplir con requisitos de seguridad que deben ser identificados desde la etapa del diseño.(aglone3, 2013)

2.1.4.9 Gestión de incidentes en la seguridad

Los sistemas de información de las organizaciones deben estar siempre monitoreados, y cualquier incidente de seguridad que se manifieste en estos, deben

ser oportunamente reportados al personal de seguridad de manera de poder tomar acciones oportunas y correctivas.

> Se debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados contratistas y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales.(ISO/IEC 27002:2005, pág. 138)

2.1.4.10 Gestión de la continuidad del negocio

Las organizaciones deben contar con un plan de continuidad del negocio (BCP) en caso de presentarse cualquier tipo de desastres como pueden ser naturales, políticos, terroristas, etc. La continuidad del negocio ayuda a reanudar los sistemas críticos de información hasta poder llegar a un nivel aceptable.(aglone3, 2013)

2.1.4.11 Cumplimiento

Los sistemas de gestión de información deben cumplir con las leyes, estatutos legales y regulatorios de las organizaciones con el fin de evitar cualquier violación de seguridad de estos.(aglone3, 2013)

2.1.5 Continuidad del negocio

En los últimos años se ha venido incrementado la continuidad del negocio en las grandes y medianas organizaciones, esto con el fin de prevenir situaciones que interrumpan las actividades normales como pueden ser

- Destrucción y daños en las instalaciones ya sea por desastres naturales (Terremotos, huracanes, inundaciones, incendios, etc.) o por factores externos (Políticos, económicos, huelgas, etc.)
- Daño en la infraestructura tecnológica, equipos de comunicación, servidores, almacenamiento, etc.
- No contar con el personal clave en situaciones extremas.
- Perdida de la información magnética como archivos físicos.
- Falta de energía eléctrica, como daño en los equipos energéticos.

Por estos y otros motivos los accionistas y dueños de las organizaciones desean diseñar, elaborar y establecer con procedimientos claros que sean difundidos a todo el personal tanto como interno como externo, si al presentarse algún incidente grave que interrumpa el normal funcionamiento de esta, se logre reestablecer en un tiempo prudente estas actividades.

2.1.6 Administración de riesgos

La administración del riesgo es una parte fundamental de las buenas prácticas y es un proceso secuencial el cual posibilita el mejoramiento continuo.
Es un método sistemático que contiene procesos de la administración de riesgo, para ello se desarrolla políticas organizacionales.(AS/NZS 4360:1999, pág. 6)

2.1.6.1 Requerimientos de administración de riesgo

2.1.6.1.1 Políticas de administración de riesgo

Por parte de la gerencia se debe determinar y poseer un respaldo físico de políticas para la administración de riesgos, definiendo los objetivos, compromisos y

garantizar el apoyo de sostener las medidas tomadas a todo el nivel de la organización.(AS/NZS 4360:1999, pág. 6)

2.1.6.1.2 Planeamiento y recursos

El proceso establecido de tener el apoyo de la alta gerencia para que pueda ser ejecutado de forma efectiva y con la suficiente firmeza para poder cumplir con las metas planteadas. (AS/NZS 4360:1999, pág. 6)

2.1.6.1.3 Programa de implementación

Todos los pasos deben ser definidos muy claramente considerando la filosofía, cultura y estructura general de administración de riesgos de la organización. (AS/NZS 4360:1999, pág. 7)

2.1.6.1.4 Revisión gerencial

La parte ejecutiva de la organización debe certificar que todo el sistema de administración de riesgos se lleve a cabo para satisfacer los requerimientos de este estándar, y las políticas y objetivos de riesgos establecidos en la organización. (AS/NZS 4360:1999, pág. 7)

2.1.6.1.5 Proceso de administración de riesgos

Se debe proceder con una secuencia de pasos para poder implementar efectivamente la administración de riesgos dentro de la organización.

El proceso de la administración de riesgos se encuentra dentro de la estructura del contenido estratégico empresarial. (AS/NZS 4360:1999, pág. 10)

2.1.6.1.6 Administración de riesgos

Relación de principios - Marco de trabajo (Framework) – Proceso de Gestión de Riesgos

Proceso de Gestión de Riesgos

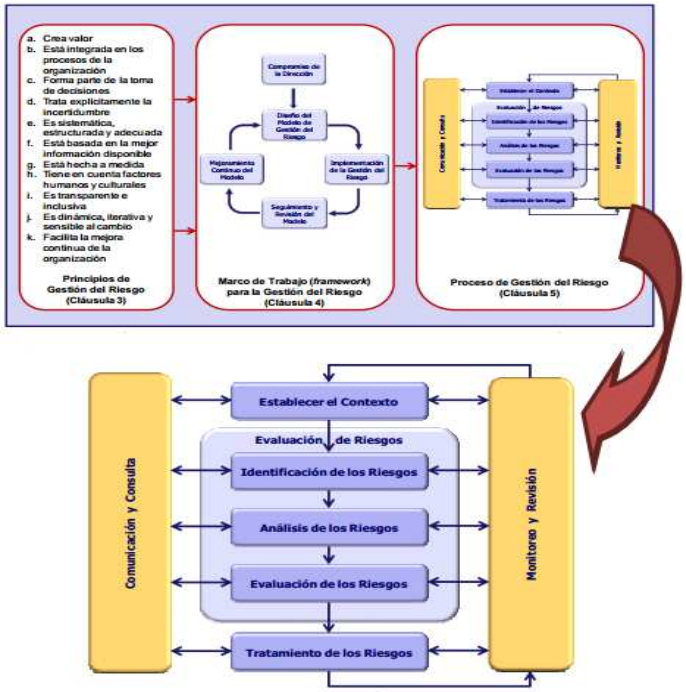

Figura 3 Forma ISO 31000 versión 2009: Gestión de Riesgos – Principios y Guías

2.1.6.1.6.1 Establecer el contexto

La organización define sus objetivos y metas a cumplir y por ellos identifica los parámetros internos y externos para la gestión de riesgos. (AS/NZS 4360:1999, pág. 10)

2.1.6.1.6.2 Establecer el contexto externo

Este tiene como objeto la verificación y orientación de la naturaleza social y cultural, política, jurídica, reglamentaria, financiera, tecnológica, económica, y entorno competitivo, ya sea internacional, nacional, regional o local.(AS/NZS 4360:1999, pág. 11)

2.1.6.1.6.3 Establecer el contexto interno

Tiene por objetivo el manejo interno de la organización, estructura organizativa, las funciones y responsabilidades. Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos los objetivos de la organización.(AS/NZS 4360:1999, pág. 11)

2.1.6.1.6.4 Identificación de riesgos

Es una de las etapas fundamentales ya que se tiene que generar una lista completa de los riesgos basados en crear, prevenir, degradar, retrasar el conseguir los objetivos y metas de la organización.

La identificación correcta de los riesgos es fundamental, ya que si no se los procesa de buena forma y no se los define estos no serán tratados y por ellos no serán analizados en los pasos siguientes en la gestión de riesgos. (AS/NZS 4360:1999, pág. 12)

2.1.6.1.6.5 Análisis de riesgos

El principio que posee este tipo de análisis es poder diferenciar los tipos de riesgos y vulnerabilidades como son, los riesgos menores aceptables y los riesgos mayores, algo fundamentales también poder obtener la información necesaria para la evaluación y el procesamiento del riesgo, y se puede identificar de buena forma los controles necesarios para mitigar o controlar el riesgo.

De esta manera se puede evaluar su probabilidad a que ocurra el evento e identificar las consecuencias.

Con el análisis se puede excluir los riesgos similares o de bajo impacto que no pueden trascender en el tiempo.

Tener una idea clara entre el tipo de riesgo y el control que se debe implementar es fundamental para los auditores de TI, ya que si no se identifica correctamente al tipo de riesgo el control o los controles que se apliquen pueden no tener el resultado deseado.

Los auditores deben conocer los riegos comunes del negocio y evaluar de forma correcta cada uno de los procesos, valoración del riesgo y la gestión de los gerentes del negocio y poder planificar el trabajo de auditoria.

La identificación de las amenazas pueden ser financieras, regulatorias como también operacionales, las cuales pueden resultar de las operaciones del negocio con su entorno o ser resultado de sus estrategias realizadas o también de los procesos, procedimientos e información utilizados por el negocio.

El auditor por lo general se encuentra enfocado en los mayores riesgos asociados con la confidencialidad, disponibilidad o integridad de la información sensible y critica, ya que en el manejo, modificación, manipulación y

almacenamiento de la información puede estar comprometida para el buen desempeño de la organización ya que sin esta información puede estar en riesgo el funcionamiento y el futuro operativo de la organización.

El proceso de evaluación posee un ciclo de vida que tiene como inicio el identificar los objetivos de la organización o negocio, los activos de información y los sistemas o recursos de información que tengan y manipulen información de vital importancia como es hardware, software, base de datos, redes, instalaciones, personas, etc.

Ya identificados los activos de información sensible o critica, se realiza una evaluación de riesgos para identificar las amenazas y poder determinar la probabilidad de ocurrencia, como el fin y dimensionar el impacto resultante y sus respectivas medidas para la mitigación de las amenazas hasta llegar a un nivel aceptable para la organización.

Se puede determinar el impacto mediante un análisis y cálculos estadísticos, cuando no se disponen de datos o informes anteriores.

Para evitar el análisis incorrecto se puede utilizar técnicas y fuentes de información disponibles las cuales se detalla a continuación:

- Registros anteriores
- Experiencias relevantes
- Prácticas y experiencias de la industria
- Literatura relevante publicada
- Comprobaciones de marketing e investigación de mercado
- Experimentos y prototipos
- Modelos económicos, de ingeniería u otros

- Opiniones y juicios de especialistas y expertos

Las técnicas pueden incluir:

- Entrevistas estructuradas con expertos en el área de interés
- Utilización de grupos multidiciplinados de expertos
- Evaluaciones individuales utilizando cuestionarios
- Uso de modelos de computadora u otros
- Uso de árboles de fallas y árboles de eventos

Ya en la etapa de mitigación del riesgo se identifican los controles para mitigar los riesgos identificados, los controles que se ponen son medidas para la mitigación del riesgo que tratan de conseguir como resultado prevenir, reducir y en los mejores de los casos eliminar la probabilidad de que el evento ocurra, detectar la ocurrencia y minimizar el impacto o transferir el riesgo.

La evaluación de los controles es uno de los pasos principales que se debe dar el interés necesario ya que se lo realiza mediante un análisis costo - beneficio hasta que tenga el riesgo un nivel aceptable por parte de la gerencia y esto se analiza de la siguiente forma:

- El costo del control comparado con el beneficio de minimizar el riesgo
- La tolerancia a riesgos de la gerencia de aceptación de la amenaza
- Métodos de preferidos de reducción de riesgos

La siguiente etapa es la última y se la conoce como monitoreo de los niveles de desempeño de los riesgos gestionados cuando se procede con cambios que son relevantes y significativos.

Estos tienen procesos de verificación que son:

- Evaluación de riesgos
- Mitigación de riesgos
- Reevaluación de riesgos

Aplicado esto podemos volver a identificar si los riesgos están en un nivel aceptable para la gerencia.

Es necesario resaltar que para tener un buen grado de efectividad la evaluación de los riesgos, debe ser un proceso continuo en una organización que se preocupe por

identificar y evaluar constantemente los riesgos a medida que estos surjan. (AS/NZS 4360:1999, pág. 13)

2.1.6.1.6.6 Tipos de análisis

El análisis de riesgo puede tener varios tipos de refinamiento dependiendo del riesgo y de la disponibilidad de datos. Dependiendo de los parámetros disponibles los análisis pueden ser, cualitativo, semicualitativo o cuantitativo o una combinación de ellos, todo depende de la complejidad y el costo de estos análisis en orden ascendente.

En primera instancia se utiliza el análisis cualitativo para obtener una idea o estado general del nivel del riesgo. (AS/NZS 4360:1999, pág. 14)

2.1.6.1.6.6.1 Análisis cualitativo

El análisis cualitativo utiliza términos subjetivos y otras con términos objetivos estas evaluaciones dependen principalmente del conocimiento y juicio de

las personas implicadas su comprensión de los eventos posibles y del entorno que lo rodea. (AS/NZS 4360:1999, pág. 14)

Tabla1 AS/NZS 4360:1999

Nivel	Descripción	Ejemplo de la descripción detallada
1	Insignificante	Sin perjuicios, baja perdida financiera
2	Menor	Tratamiento de primeros auxilios, liberado localmente se contuvo inmediatamente, pérdida financiera media
3	Moderado	Requiere tratamiento médico liberado localmente considerado con asistencia externa, perdida financiera alta
4	Mayor	Perjuicios extensivos, perdida capacidad de producción, liberación externa, sin efectos nocivos, pérdida financiera mayor
5	Catastrófico	Muerte, liberación toxica externa con efectos nocivos enorme pérdida financiera

2.1.6.1.6.6.2 Análisis semi-cuantitativo

La escala semi-cuantitativa se les asigna valores, el cual no tiene relación directa con la magnitud real, lo que trata es de dar a mayor detalle evaluando con números y combinándolos.

Es importante tener en cuenta el uso de esta técnica ya que por los números seleccionados no se podría tener una evaluación correcta y real del riesgo. (AS/NZS 4360:1999, pág. 15)

2.1.6.1.6.6.3 Análisis cuantitativo

Utiliza valores números con una escala definida dependiendo del riesgo y estos son descritos utilizando distintos orígenes de datos.

La exactitud del análisis dependerá de la precisión e integridad de los valores numéricos utilizados y pueden ser catalogados de los estudios y datos realizados anteriormente. (AS/NZS 4360:1999, pág. 15)

2.1.6.1.7 Evaluación de riesgos

La evaluación del riesgo tiene como objetivo ayudar a decidir de mejor manera el tratamiento y la prioridad que se debe implementar según el análisis de riesgos realizado anteriormente.

Las acciones que se va a tomar deben considerar los riesgos tolerables ya los que se asumen, son definidos mediante el beneficio que se tiene a la organización. Las decisiones que se determinan van de acuerdo a los requisitos legales y reglamentos internos y externos de la organización. (AS/NZS 4360:1999, pág. 15)

2.1.6.1.8 Tratamiento de los riesgos

El tratamiento del riesgo consiste en realizar diferentes procesos para modificar el estado del riesgo.

- El proceso de tratamiento del riesgo tiene varias etapas:
- Examinar el tratamiento del riesgo
- Decidir los niveles residuales es tolerables de aceptación del riesgo.

Si los riesgos no son tolerables estos deben ser generados con un nuevo riesgo.

Las opciones que se puede tomar para el tratamiento del riesgo son:

- Evitar el riesgo.
- Tomar o aumentar el riesgo
- Eliminar el riesgo, mitigando su origen
- Cambiar su probabilidad
- Cambiar las consecuencias
- Distribuir el riesgo

- Mantener el riesgo

(AS/NZS 4360:1999, pág. 16)

2.1.6.1.9 Selección del tratamiento del riesgo

La selección de la mejor forma de tratar o mitigar un riesgo debe estar acorde con los costos y el trabajo que representa, contra el beneficio que se obtiene al tratar dichos riesgos, los cuales deben estas dentro de las normas legales y reglamentos de la organización.

La toma de decisiones deben estar precedida por todas las personas involucradas del riesgo y de la mitigación.

El plan de tratamiento del riesgo debe estar definido a detalle y especificado el problema y su prioridad conjuntamente con el tratamiento individual.

El tratamiento de los riesgos puede generar riesgos segundarios, que deben ser evaluados y si lo amerita deben ingresar como un riesgo nuevo y ser incorporado en el plan de tratamiento según su prioridad.(AS/NZS 4360:1999, pág. 16)

2.1.6.1.10 Monitoreo y revisión

El seguimiento y la revisión deben tener una planificación dentro de los planes de la organización, ya que cada una de las diferentes acciones tomadas les corresponde ser evaluadas y se considera la revisión y monitoreo respectivo.

Todas las actividades deben ser establecidas con claridad y registradas por si existiese algún tipo de problema.

Una de las partes exitosas que tiene la revisión de los controles, es verificar la eficiencia y eficacia de estos, tanto en el diseño como en su ejecución.(AS/NZS 4360:1999, pág. 19)

2.1.6.1.11 Registro del proceso de gestión de riesgo

Cada uno de los cambios y resultados deben ser registrados en una bitácora para poder utilizarlos, ya que son muy importantes para la organización para el aprendizaje continuo.

Se promueve el crecimiento y mantenimiento de registros.

2.1.6.1.12 Comunicación y consulta

Esta parte es muy importante en el proceso, ya que se debe comunicar a todos los involucrados ya sean internos o externos, que se podrían tomar con un punto de referencia cuestionarios relacionados con el riesgo en sí mismo, sus causas, consecuencias y las medidas que se proponen para mitigarlas.

Esta comunicación tanto interna como externa debe ser efectiva ya que garantiza las responsabilidades en el proceso de gestión de riesgo.

Un principio fundamental de la comunicación es visualizar de mejor forma un contexto adecuado que los riesgos si estos están plenamente identificados, apoyar de buena forma el plan de tratamiento.

2.1.3.7 Auditoria

La auditoría en informática es el proceso que se basa en normas, procesos y técnicas definidas de recolección y evaluación de evidencias para determinar

cuando son salvaguardados los activos de los sistemas computarizados, de qué manera se mantiene la integridad de los datos y como se logran los objetivos de la organización eficazmente y se usan los recursos consumidos eficientemente. La auditoría en informática sigue los objetivos tradicionales de la auditoria: aquellos que son de la auditoria externa, de salvaguarda de los activos y la integridad de datos y los objetivos gerenciales, aquellos propios de la auditoria interna que no solo logran los objetivos señalados si no también los de eficiencia y eficacia. (Echenique, 2008, p.26)

2.1.7 Auditoria informática

Consta de una gran importancia se basa en el principio de evaluar de forma sistemática y objetiva, es un parte integral de la Auditoria, en fin es definir el uso adecuado y como son utilizados los recurso informáticos.

2.1.7.1 Objetivo de la auditoria informática

- De los hallazgos encontrados presentar recomendaciones para que pueda tomase correctivos adecuados.
- Verificar si la información que es adquirida y procesada por parte de los sistemas informáticos es correcta y cumpla con las necesidades que requiere la institución.
- Comprobar si se da el debido proceso en la creación de un nuevo aplicativo.
- Evidenciar si se cumple o no las políticas, procesos y normas que se tienen establecidas por parte de la Institución.

2.1.7.2 Tipos de auditoria

Existe dos tipos las cuales por la utilización del talento humano se clasifican como:

Auditoria interna: Es cuando se procede a realizar la auditoria con personal que labore en el establecimiento o institución.

Auditoria externa: El procedimiento es realizado por una firma auditora externa la cual no tiene ningún recurso humano dependiente de la institución que va hacer auditada.

2.1.7.3 Auditoría informática externa

Las Instituciones recuren a una firma auditora por algunos motivos importantes como es:

- Descoordinación de los procesos
- Financiamiento económico
- Por la reputación y claridad de los procesos auditados

2.1.7.4 Auditoría informática de desarrollo de aplicaciones

Para la creación de un aplicativo en cada una de las fases de desarrollo debe llevar un control eficiente por la parte económica, como también en la parte de cumplir con las necesidades requeridas y en los plazos acordados.

2.1.7.5 Auditoría de los datos de entrada

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que

los controles de integridad y calidad de datos se realizan de acuerdo a las Normas establecidas.

El ingreso de la información debe ser compatible con los sistemas teniendo por meta el cumplimiento de tiempos, procesamiento de datos y sobre todo que cumplan con el CID (Confiabilidad, Integridad y disponibilidad), que es vital para el manejo de datos.

- Sistema Operativo: Identificar que no se tengan problemas con el sistema base.
- Software de Aplicación: Valorar las aplicaciones desarrolladas.
- Comunicaciones: Comprobar que el rendimiento de la red sea adecuado y pueda sumar le valor a la institución.

2.1.7.6 Fases de la auditoria informática

- Fase I: Conocimientos del Sistema
- Fase II: Análisis de transacciones y recursos
- Fase III: Análisis de riesgos y amenazas
- Fase IV: Análisis de controles
- Fase V: Evaluación de Controles
- Fase VI: El Informe de auditoria
- Fase VII: Seguimiento de las Recomendaciones

2.1.7.6.1 Fase I Conocimientos del sistema

Aspectos Legales y Políticas Internas.

Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.

2.1.7.6.1.1 Características del sistema operativo.

- Organigrama del área que tengan alguna relación con el aplicativo desarrollado.
- Poseer un manual de uso
- Histórico de auditorías realizadas antes.

2.1.7.6.1.2 Características de la aplicación de computadora

- Manual técnico del aplicativo o sistema
- Documento donde constes las funciones y personal capacitado para su administración.
- Descripción de equipos en el cual corre el aplicativo
- Seguridad en las claves de acceso al sistema como a su configuración
- Generación de almacenamiento y procesamiento esperado.

2.1.7.6.2 Fase II Análisis de transacciones y recursos

2.1.7.6.2.1 Definición de las transacciones.

El grado de complejidad del sistema se divide en dos grupos procesos y subprocesos todos dependiendo de grado de complejidad tenga.

2.1.7.6.2.2 Análisis de las transacciones

- Establecer el flujo de los documentos que intervienen en los diferentes procesos

Es de forma obligatoria el tener bien definido en un flujograma el funcionamiento y los diferentes estados de un proceso.

2.1.7.6.2.3 Análisis de los recursos

Determinar el recurso necesario que interviene y es en el sistemas cuales son los procesos definidos de forma específica.

2.1.7.6.3 Fase III: Análisis de riesgos y amenazas

2.1.7.6.3.1 Identificación de riesgos

- Problemas que se pueden presentar en los diferentes recursos
- Conflicto de seguridad que no sea tomados como prioridad
- Desconcierto por el proceso claro que conlleva a la perdida de documentos o fuentes requeridos por los procesos.
- No poseer un registro de Errores

2.1.7.6.3.2 Identificación de las amenazas

Las amenazas puede presentarse de diferentes formas como es en los equipos, información o aplicativos.

2.1.7.6.4 Fase IV: Análisis de controles

2.1.7.6.4.1 Codificación de controles

Los controles se son determinados e identificados por el grupo al que pertenecen.

2.1.7.6.4.2 Análisis de cobertura de los controles requeridos

Se determina que el control cubra todo el campo que el auditor requiere ya que si es escogido de mala forma el control no podrá dar el buen resultado que se espera.

2.1.7.6.5 Fase V: Evaluación de controles

2.1.7.6.5.1 Objetivos de la evaluación

Comprobar la presencia de los controles que se requiere para cada proceso.

Identificar el buen funcionamiento del control.

2.1.7.6.5.2 Plan de pruebas de los controles

- Se debe realizar pruebas para determinar si cubre el objetivo deseado el control.
- Para realizar pruebas se debe solicitar datos casi reales para poder contar con una aproximación adecuada a la eficiencia del control.

2.1.7.6.5.3 Pruebas de controles

- Cada uno de los resultados deben ser documentados y registrado en un bitácora

2.1.7.6.5.4 Análisis de resultados de las pruebas

- Cada uno de los resultados debe ser evaluado y si no cumplen, se debe volver a estructura el control y evaluarlo otra vez.

2.1.7.6.6 Fase VI: Informe de auditoria

2.1.7.6.6.1 Informe detallado de recomendaciones

- Él informa detallado se lo debe definir de forma clara y con los respaldos que lo sustenten

2.1.7.6.6.2 Evaluación de las respuestas

- Se recomienda sustentarse en la ley de la organización y los objetivos del negocio.

2.1.7.6.6.3 Informe resumen para la alta gerencia

Este informe debe prepararse una vez revisadas las respuestas por cada área y definidas el de compromiso de las mismas.

Para lo cual debe contar de:

Introducción: objetivo y contenido del informe de auditoria

Objetivos de la auditoría

Alcance: cobertura de la evaluación realizada

Hallazgos

Recomendaciones

2.1.7.6.7 Fase VII: Seguimiento de recomendaciones

Informes del seguimiento

Evaluación de los controles implantados

Capítulo III

3.1 Metodología de Investigación

3.1.1 Ubicación geográfica del proyecto de investigación.

País: Ecuador.

Provincia: Pichincha - Distrito Metropolitano de Quito, Centro histórico, Venezuela N3-86 y Espejo.

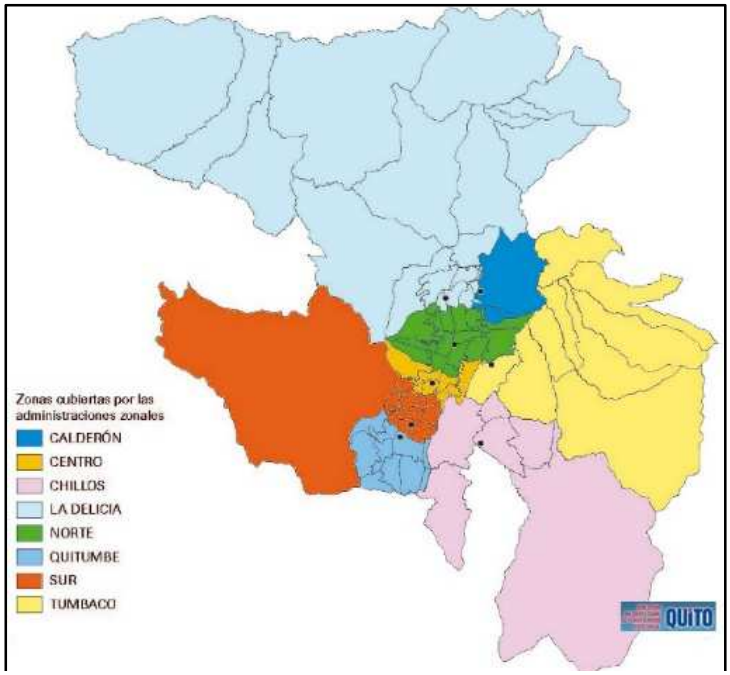

Figura 4. Mapa del Distrito Metropolitano de Quito
Fuente: Dirección Metropolitana de Planificación Territorial, 2013

3.1.2 Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información

En el presente desarrollo de la tesis, se utiliza una metodología basada en riesgos, utilizando métodos de investigación de fuentes primarias como son encuestas, entrevistas y observación.

CAPÍTULO IV

4.1 Evaluación técnica del Data Center

4.1.1 Situación actual

El eje tecnológico del Municipio del Distrito Metropolitano de Quito (MDMQ) es la Dirección Metropolitana de Informática (DMI), su principal objetivo es proporcionar a la organización las herramientas necesarias que le permitan soportar, desde la perspectiva tecnológica, la operación de los procesos Municipalidad de forma eficiente.

4.1.1.1 Misión

> La DMI tiene como Misión proveer soluciones integrales, a través de las tecnologías de información y comunicación (TIC´s) para la gestión del MDMQ, enfocado en servir a la ciudadanía, mediante la utilización de herramientas informáticas que nos permitan desarrollar proyectos tecnológicos para implementar e innovar procesos, que garanticen la disponibilidad, integridad, seguridad y confiabilidad de la información, con el soporte de un equipo humano profesional altamente capacitado, involucrado y comprometido.(PETI DMI, pag6)

4.1.1.2Visión

> La DMI al 2015 se proyecta como la dependencia asesora, rectora y referente dentro del MDMQ, en temas de software, hardware, telecomunicaciones y proyectos. Promoviendo el uso efectivo y eficiente de las tecnologías de información y comunicación para contribuir al desarrollo organizacional en beneficio de la ciudadanía. (peti DMI, pag6)

4.1.1.3Cadena de valor

A continuación se describe la cadena de valor de la DMI

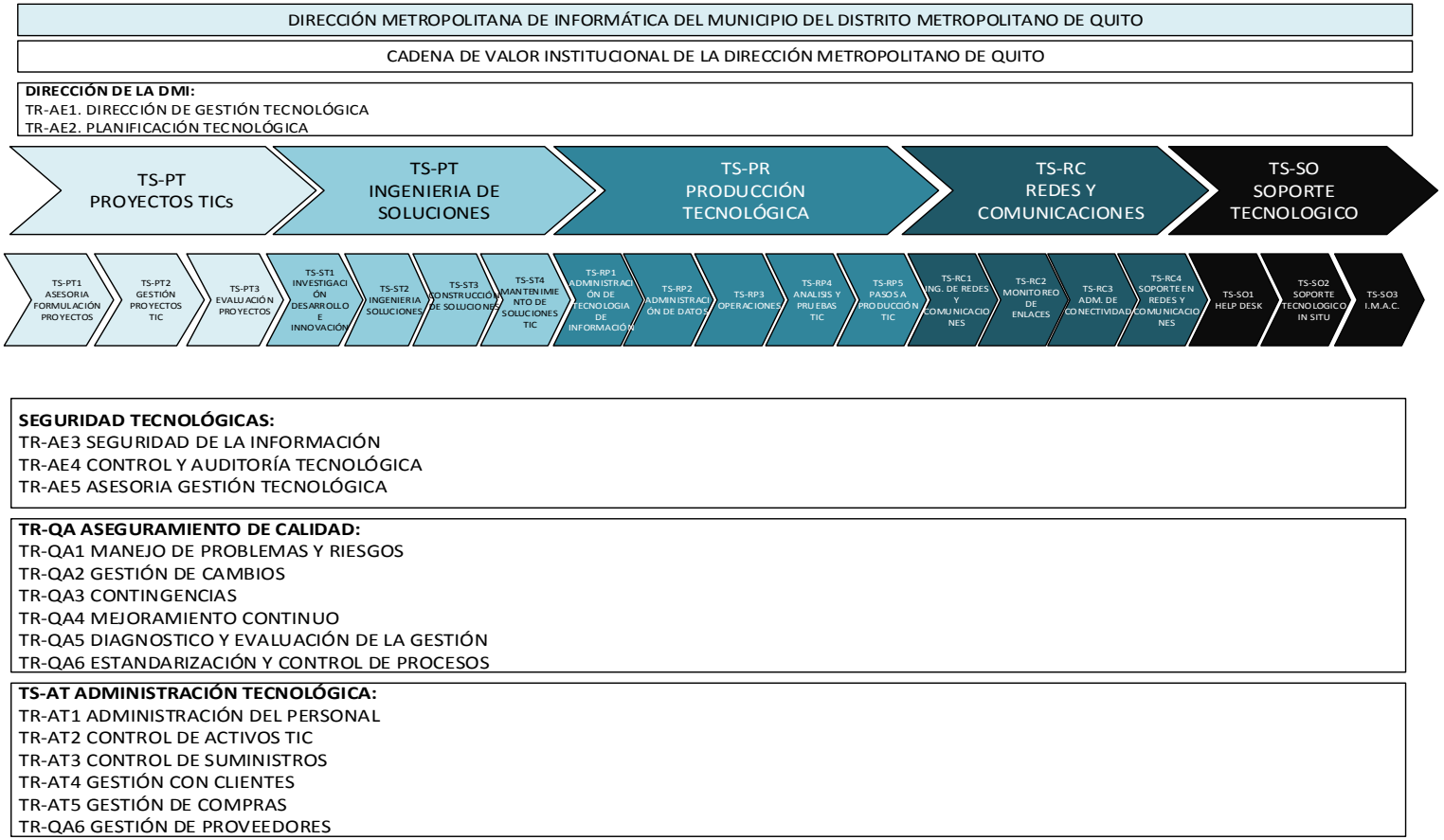

Figura 5 Cadena de Valor Dirección de Informática

4.1.2 Actividad de la DMI

El MDMQ 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,

El MDMQ, dentro del su plan Metropolitano de Desarrollo establece ejes estratégicos que permitan estructurar de manera integral, articulada, sistemática las proyecciones de desarrollo con proyección hacia el 2022; el mismo 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 DMI como el ente rector para emitir políticas que apoyen a la Gestión Tecnológica. (Ordenanza N0170,2012)

4.1.3 Actividades de la Dirección Metropolitana de Informática (DMI)

La DMI se encuentra en el nivel de gestión brinda fundamentalmente servicios tecnológicos confiables, seguros y eficientes para ayudar a explotar y mejorar los procesos institucionales, que los ofrece tanto al usuario interno como a la ciudadanía.

4.1.4 Orgánico funcional del Municipio del Distrito Metropolitana de Quito (MDMQ)

A continuación se presenta en la figura 6, todos los niveles que estructura el orgánico Funcional del MDMQ.

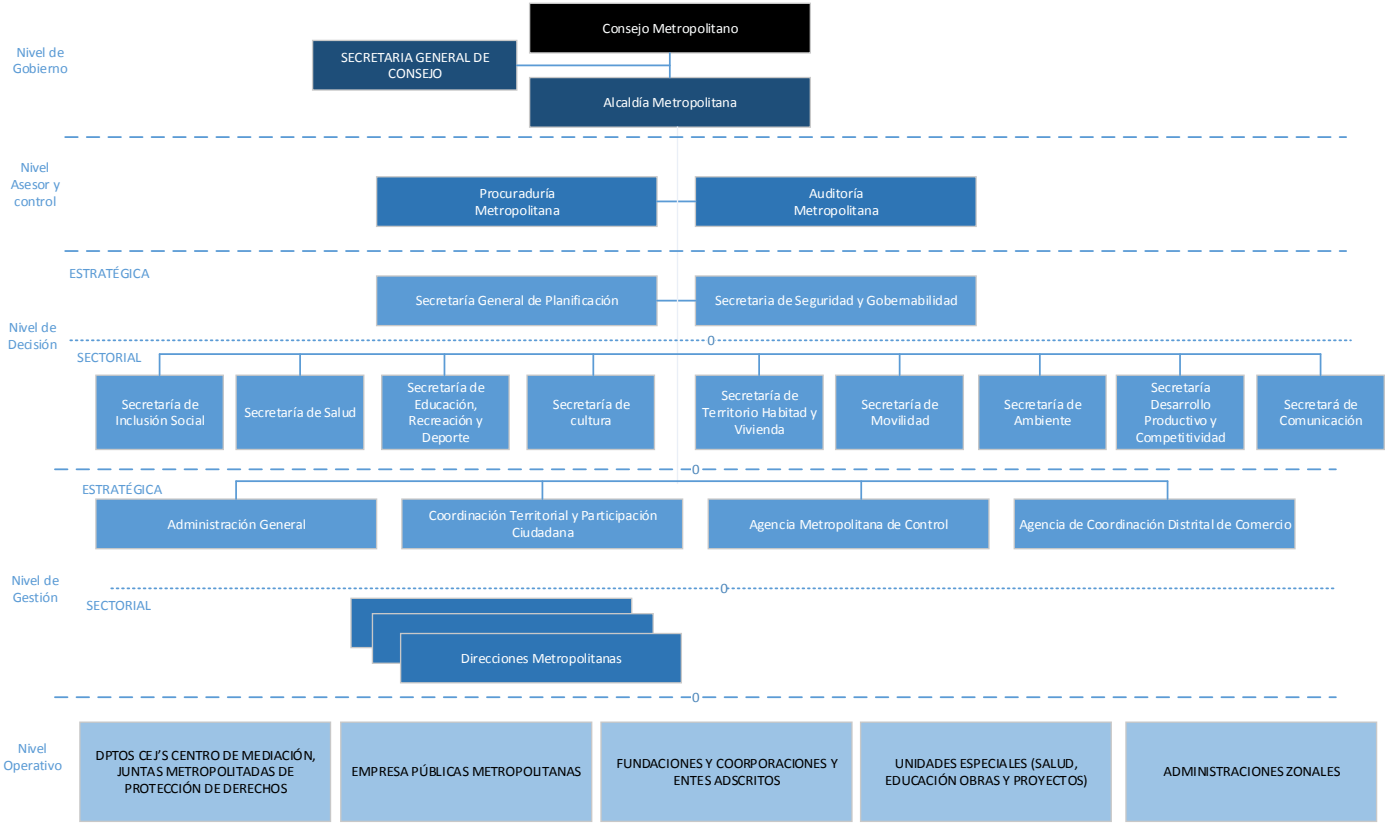

Figura 6 Orgánico Funcional MDMQ

4.1.5 Orgánico funcional DMI

En la figura 7 se presenta los departamentos que conforman la DMI

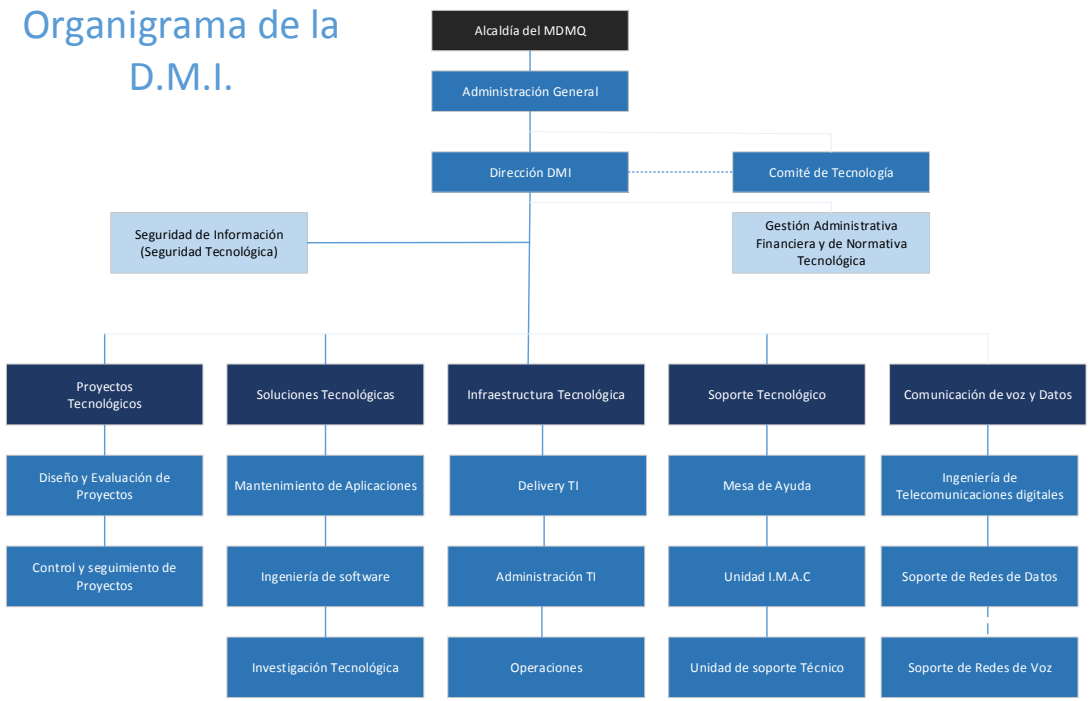

Figura 7 Orgánico Funcional DMI

Fuente: Plan estratégico de tecnologías de información, 2011

4.1.6 Estructura interna de la DMI

4.1.6.1 Seguridad de información

Es la unidad de la DMI, la cual establece mecanismos que protegen y salvaguardan la información contra pérdidas, fugas, robo y alteración de la información que es procesada en el MDMQ. Es encargada de dictar, ejecutar y dar cumplimiento a las políticas de seguridad de la información para todo el MDMQ.

4.1.6.2 Área de proyectos

En la Dirección de Informática se encuentra en su organigrama el área de proyectos la misma que es la encargada de la gestión de proyectos tecnológicos. Está constituida por dos sub áreas las mismas que son:

4.1.6.2.1 Diseño y evaluación de proyectos

Un proyecto nace cuando se firma un contrato no obstante en el MDMQ, existen varias acotaciones y es necesario realizar un diseño por esta razón se ha creado una sub área la misma que se encarga del estudio de proyectos, el mismo que abarca las siguientes fases: estudio de factibilidad económica, evaluación, aprobación, todo lo que es análisis arquitectura y elaboración de términos de referencia, procesos de contratación, verificación de la documentación correspondiente y seguimiento del plan de trabajo.

4.1.6.2.2 Ejecución de proyectos

Se encarga específicamente la implementación de los proyectos con las áreas de producción, ingenierías de soluciones, redes y telecomunicaciones, soporte técnico y con los proveedores para la instalación de equipos desarrollo de software e instalación de aplicaciones que son parte del plan anual de compras de la DMI y de las líneas estratégicas que vienen de la alcaldía.

4.1.6.3 Comunicación de voz y datos

4.1.6.3.1 Ingeniería de telecomunicaciones digitales

Controla los protocolos de los sistemas de transmisión de datos, redes de Área Local (LAN), Redes de Área Metropolitanas (WAN) y la red digital de servicios integrados de todos los entes del MDMQ.

4.1.6.3.2Soporte de redes de datos

Monitoreo y gestión de redes, monitoreo de los enlaces y equipos de comunicaciones, soporte técnico de la seguridad, redes inalámbricas, redes cableadas.

4.1.6.3.3 Soporte de redes de voz

Monitorea y opera en a lo referente a las comunicaciones y equipos de voz sobre IP en el MDMQ.

4.1.6.4 Infraestructura tecnológica

4.1.6.4.1 Delivery TI

Gestiona el versiona miento de las aplicaciones, sistemas, base de datos, proyectos tecnológicos, etc. Gestión para el aseguramiento de la calidad del software y hardware.

4.1.6.4.2 Administración TI

Apoya y da soporte a las áreas técnicas del MDMQ en el ámbito de los servidores y servicios informáticos. Ejecuta procedimientos para la resolución de problemas en el ámbito de los servidores y servicios informáticos. Elabora especificaciones técnicas para los proyectos de tecnología. Participa en los equipos de desarrollo de los proyectos de tecnología. Elabora y actualiza planes de contingencia de la infraestructura de servidores y servicios informáticos.

4.1.6.4.3 Operaciones

Verifica, mantiene y garantiza la operatividad y disponibilidad de la infraestructura y los servicios informáticos. Se encarga de monitorear las actividades de la infraestructura informática, mantiene y actualiza bitácoras de operación de toda la infraestructura del centro de cómputo y son los encargados de la ejecución de procesos las 24 horas.

4.1.6.5 Departamento de soluciones tecnológicas

4.1.6.5.1 Mantenimiento de aplicaciones

Departamento orientado a generar alcances de los sistemas de información que se encuentran en producción con nuevas mejoras. Estos cambios se pueden producir por el cambio de la parte legal, por nuevos requerimientos o mejoras al producto actual.

4.1.6.5.2 Ingeniería de software

Orientado de la generación de producto para los diferentes entes del municipio para la automatización de sus procesos. Además de dar seguimiento de contrataciones de nuevos sistemas solicitado por los entes Municipales

4.1.6.5.3 Investigación tecnológica

Orientada a adquirir conocimiento de las nuevas herramientas que existen en el mercado y fortalecer el conocimiento ya adquirido con metodologías formales.

4.1.6.6 Soporte tecnológico

4.1.6.6.1 Mesa de ayuda

Se encarga del levantamiento de requerimientos tecnológicos por parte de los usuarios internos del municipio además de dar seguimiento a estos para su cumplimiento.

4.1.6.6.2 Unidad de soporte técnico

Se encarga en el soporte en sitio, de los incidentes de hardware y software reportados por los usuarios internos.

4.1.6.6.3 Unidad I.M.A.C

Encargada de realizar mantenimiento preventivo de los equipos informáticos de las diferentes dependencias municipales.

Realizar mantenimiento correctivo, realizar la reparación y puesta en marcha de equipos computacionales que presenten fallas en su funcionamiento, procurando la eficiencia y un oportuno servicio.

Realizar instalaciones eléctricas y de datos en poca escala.

Movilizar equipos y mantener control a través del registro de la entrada y salida de los equipos de computación.

Coordinar con la Organización privada la reparación de equipos de computación que no se efectúan en el departamento de Administración de Equipos Informáticos

4.1.7 Data Center del MDMQ

El Data Center del MDMQ esta ubicación en el primer piso del Edificio de Avalúos y Catastros localizado en la calle Venezuela N3-86 y Sucre.

Dentro del data center encontramos servidores blades de tipo rack y torre, almacenamientos, enclouser, UPS, KVM, centrales telefónicas, switch de tipo LAN y SAN, routers, sistemas de extintores, aire acondicionado, tablero de distribución eléctrico, cámaras de seguridad, etc. entre sus principales elementos.

4.1.8 Tabla de elementos del data center

Se ha obtenido un listado de los elementos que mayor mente integran el data center del MDMQ como son: Aplicaciones que son utilizadas tanto por los clientes internos como externos, servicios contratados (externos), infraestructura que compone el data center, equipos de red, servidores físicos como virtuales, personal que trabaja en el center. Toda esta información fue obtenida en conjunto por todos los responsables que interactúan directamente en el data center.

4.1.8.1 Listado de aplicaciones del MDMQ

Esta primera tabla está conformada de columna 1 es conformada 82 aplicaciones que se manejan en el MDMQ. Columna 2 Código que representa a los aplicativos está conformado con la letra A y un consecutivo numérico. Columna 3 número aproximado de usuarios que se verían afectados por la fallas en los aplicativos. Columna 4 impacto que se califica al aplicativo cuando este deje de funcionar o presente alguna falla el cual no permita su correcto funcionamiento. Columna 5 probabilidad que significa que tan posible es que se presente la falla del aplicativo. Columna 6 riesgo que se obtendrá de la multiplicación del impacto por la probabilidad

4.1.8.2 Calificación del impacto a las aplicaciones del MDMQ

Se ha manejado una escala del 1 al 5 para la calificación al impacto a las aplicaciones cuando esta deja funcionar o tiene una interrupción

Donde:

Valor = 1 representa un impacto bajo al momento de la interrupción o falla de operación del aplicativo, el funcionamiento de aplicativo se lo puede restaurar en un tiempo de 1 a 5 minutos. Valor = 2 representa un impacto moderado al momento de la interrupción o falla de operación del aplicativo, el funcionamiento de aplicativo se lo puede restaurar en un tiempo de 5 a 15 minutos. Valor = 3 es un impacto medio al momento de la interrupción o falla de operación del aplicativo, el funcionamiento de aplicativo se lo puede restaurar en un tiempo de 15 a 30 minutos. Valor = 4 un impacto alto al momento de la interrupción o falla de operación del aplicativo, el funcionamiento de aplicativo se lo puede restaurar en un tiempo de 30 minutos a 2 horas. Valor = 5representa un impacto catastrófico al momento de la interrupción o falla de operación del aplicativo, el funcionamiento de aplicativo se lo puede restaurar en un tiempo de 2 horas a 3 días.

Tabla 2 Escala de impacto de aplicaciones del MDMQ

Valor	Escala de Impacto
1	Bajo
2	Moderado
3	Medio
4	Alto
5	Catastrófico

4.1.8.3 Calificación de la probabilidad de falla para las aplicaciones del MDMQ

Se ha manejado una escala del 1 al 4 la priorización del impacto

Donde:

Valor = 1 representa la probabilidad baja de producirse la falla del aplicativo. Valor = 2 representa la probabilidad media de producirse la falla del

aplicativo. Valor = 3 una probabilidad alta de producirse la falla del aplicativo. Valor = 4 una probabilidad catastrófica de producirse la falla del aplicativo.

Tabla 3 Escala de probabilidad a las aplicaciones del MDMQ

Valor	Escala de Probabilidad
1	Bajo
2	Medio
3	Alto
4	Catastrófico

4.1.8.4 Priorización del riesgo

Para establecer el riesgo se maneja tres escalas para la priorización del riesgo

Donde:

Riesgo 1 > = 5 son riesgos bajos, cuando un aplicativo fallará. Riesgo 6 > = 10 riesgos medios, cuando un aplicativo fallará. Riesgo 11 > = 15 altos, cuando un aplicativo fallará. Riesgo 16 > = 20 Catastróficos, cuando un aplicativo fallará.

4.1.8.5 Tabla de riesgo

Se construye dicha tabla tomando la relación entre riesgo e impacto, en el eje vertical se ubica el impacto y el eje horizontal el riesgo y en cada cuadrante según la escala se encuentran las aplicaciones que posee la MDMQ.

4.1.8.6 Listado de aplicaciones del MDMQ

Tabla 4 Listado de Servicios pertenecientes al M.D.M.Q

Escala de Impacto	Escala de Probabilidad
1 Bajo	1 Bajo
2 Moderado	2 Medio
3 Medio	3 Alto

Continúa…

4 Alto	4 Catastrófico
5 Catastrófico	

Servicio Informático	Código	Número de Usuarios	Impacto	Probabilidad	Riesgo
Sistema de Pagos de Impuestos a través de la Banca y Cooperativas	A1	3000	4	2	8
Sistema Integrado de Registro Catastral de Quito - SIRECQ	A2	500	4	2	8
Sistema de Pagos de Impuestos a través de tarjetas de Crédito	A3	3000	4	2	8
Sistema de Seguridad y Personas	A4	500	3	2	6
Sistema SAO	A5	500	3	2	6
LUAE - BPM	A6	400	3	2	6
Sistema de Administración de Requerimientos - GDOC	A7	300	3	2	6
Sistema Territorial IRM Informe Regulación Metropolitana	A8	200	3	2	6
Sistema Territorio SGCT Sistema de gestión de la Construcción Territorial	A9	200	3	2	6
SAO-Patentes	A10	500	3	2	6
Rehosting	A11	100	3	2	6
SISTEMA SIABIM	A12	60	3	2	6
Sistema SIABIP	A13	100	3	2	6
Directorio Activo	A14	8000	5	1	5

Continúa…

Sistema Financiero As400	A15	8000	4	1	4
Sistema Registro Civil	A16	50	2	2	4
Sistema de Comercialización	A17	40	2	2	4
Coactivas	A18	40	2	2	4
Correo Electrónico	A19	5000	3	1	3
Servicio de Internet	A20	4000	3	1	3
Sistema Consultas Recaudación	A21	20000	3	1	3
Sistema Territorial ICUS Informe de Compatibilidad de Uso de Suelos	A22	800	3	1	3
Office Comunicaror Server (OCS)	A23	5000	3	1	3
Sistema de Cartografía - MapGuide	A24	100	3	1	3
Automatización de Procesos – Skelta Procuraduría	A25	45	3	1	3
Automatización de Procesos - Skelta Dirección Metropolitana Tributaria (DMT)	A26	30	3	1	3
Automatización de Procesos - Skelta Bienes Inmuebles	A27	35	3	1	3
Espectáculos públicos	A28	20	3	1	3
HelpDesk Authority	A29	120	3	1	3
Sistema de Administración del Recurso Humano – SIARH	A30	3000	3	1	3

Continúa …

Sistema Territorial SRCI Sistema de Reconocimiento de la construcción Informal	A31	1500	3	1	3
Sistema de Indicadores Ambientales del Distrito (SIAD)	A32	60	3	1	3
Consultas de Impuestos Web	A33	35000	3	1	3
Seguros de Vida	A34	30	3	1	3
Transferencias Financieras	A35	20	3	1	3
Office Comunicator 2da Fase - VoIP OCS	A36	5000	3	1	3
TecSultWebService carga de información.	A37	5000	3	1	3
Antispam	A38	5000	3	1	3
Wsus	A39	5000	2	1	2
Sistema REGISTRO DE LA PROPIEDAD	A40	100	2	1	2
Sistema de Control de Asistencias de RRHH	A41	50	2	1	2
Sistema Conflictos SOCIALES	A42	35	2	1	2
Integración Recaudación Financiero	A43	40	2	1	2
Sistema Movilidad	A44	100	2	1	2
Sistema de Capacitación Municipal - SICAP	A45	40	2	1	2
Portal del Instituto de Capacitación Municipal - ICAM	A46	120	2	1	2

Continúa…

Sistema Quito Avanza	A47	40	2	1	2
Sistema de Comercio Popular	A48	40	1	2	2
VPN Banco Central	A49	50	1	2	2
Calculadora Avalúos	A50	40	2	1	2
QlikView - Administradores de Flujo de Colas MDMQ	A51	5	2	1	2
QlikView - Control Interno	A52	5	2	1	2
QlikView - Cuadro de mando Cartera Vencida	A53	10	2	1	2
QlikView - Cuadro de Mando SISREG (Producción)	A54	10	2	1	2
Productividad proceso de recaudación	A55	15	2	1	2
QlikView - Recaudación MDMQ	A56	20	2	1	2
Sistema de Control de Construcciones	A57	70	2	1	2
Portal Radio Municipal	A58	20	2	1	2
Sistema Plan Anual de Compras - ePAC	A59	15	2	1	2
Sistema Unidad Ejecutora Regula tu Barrio	A60	30	2	1	2
Sistema Auditorias	A61	30	2	1	2
Consulta Bienes	A62	80	2	1	2
Portal Interno del Distrito Metropolitano de Quito INTRANET	A63	5000	2	1	2

Continúa…

Sistema Convenios	A64	45	2	1	2
Bienes Muebles Municipales	A65	100	2	1	2
Antivirus para usuarios finales ESET Smart	A66	5000	2	1	2
Antivirus para servidores Symantec	A67	200	2	1	2
Streaming - Sesiones Consejo	A68	120	2	1	2
Streaming - Online	A69	120	2	1	2
Sistema Cuadres Bancarios	A70	10	2	1	2
QMATIC	A71	15	2	1	2
Sistema TOC	A72	20	2	1	2
Sistema Sumaq	A73	35	2	1	2
QlikView - Cuadro de Mando Servicios Catastrales	A74	8	1	1	1
QlikView - Tablero de Control LUAE	A75	7	1	1	1
Gestión de Archivos	A76	100	1	1	1
Geosever	A77	20	1	1	1
Propiedad Inmueble Municipal	A78	80	1	1	1
Sistema Legal de Fiel Magister	A79	10	1	1	1
Sistema Museos	A80	70	1	1	1
Kioscos Informativos/Consulta Touch	A81	20	1	1	1
Unidad ABC(Becas)	A82	200	1	1	1

4.1.8.7 Listado priorizados de servicios según su riesgo.

En la siguiente tabla indica los aplicativos del MDMQ calificados con riesgos medio, alto o catastrófico, descartando los de riesgo bajo.

Tabla 5 Listado de Servicios Priorizados

Servicio Informático	Código	Número de Usuarios	Impacto	Probabilidad	Riesgo
Sistema de Pagos de Impuestos a través de la Banca y Cooperativas	A1	3000	4	2	8
Sistema Integrado de Registro Catastral de Quito - SIRECQ	A2	500	4	2	8
Sistema de Pagos de Impuestos a través de tarjetas de Crédito	A3	3000	4	2	8
Sistema de Seguridad y Personas	A4	500	3	2	6
Sistema SAO	A5	500	3	2	6
LUAE - BPM	A6	400	3	2	6
Sistema de Administración de Requerimientos -	A7	300	3	2	6
Sistema Territorial IRM Informe Regulación Metropolitana	A8	200	3	2	6
Sistema Territorio SGCT Sistema de gestión de la Construcción Territorial	A9	200	3	2	6
SAO-Patentes	A10	500	3	2	6
Rehosting	A11	100	3	2	6
SISTEMA SIABIM	A12	60	3	2	6
Sistema SIABIP	A13	100	3	2	6

4.1.8.8 Tabla de intervalos de riesgos de servicios del MDMQ

Se presenta la tabla de riesgos para los aplicativos

Tabla 6 Intervalos de Riesgos para servicios

Tabla de Riesgos	
Riesgo 1 > = 5	Bajo
Riesgo 6 > = 10	Medio
Riesgo 11 > = 15	Alto
Riesgo 11 > = 15	Catastróficos

4.1.8.9 Tabla de riesgos de Aplicaciones del MDMQ

El diagrama de la tabla de riesgos, se conforma ubicando los códigos de las aplicaciones en los cuadrantes correspondientes según su impacto y probabilidad.

Tabla 7 Impacto vs Probabilidad de Servicios del MDMQ

	5 catastrófico	A14			
	4 alto	A15	A1,A2,A3		
Impacto	3 medio	A19,..,A38	A4,..,A13		
	2 moderado	A39,..,A73	A16,..,A18		
	1 bajo	A74,..,A82			
		1 bajo	2 medio	3 Alto	4 Catastrófico
		Probabilidad			

4.1.8.10 Listado del equipamiento del MDMQ

Esta primera tabla está conformada de Columna 1 conformada 20 elementos que conforman el data center del MDMQ. Columna 2 Código que representa al equipamiento del data center está conformado por la letra l y un número consecutivo. Columna 3 impacto que se califica si un equipo del data center deje de funcionar o presente alguna falla el cual no permita su correcto funcionamiento. Columna 4 probabilidad que significa que tan posible es que se presente la falla del

equipo. Columna 5: riesgo que se obtendrá de la multiplicación del impacto por la probabilidad.

4.1.8.11 Calificación del impacto al equipamiento del data center MDMQ

Se ha manejado una escala del 1 al 5 para la calificación al impacto a relación cuando un equipo deja de funcionar.

Donde valor = 1 representa un impacto bajo al momento de la interrupción o falla de operación del equipamiento. Valor = 2 representa un impacto moderado al momento de la interrupción o falla de operación del equipamiento. Valor=3 es un impacto medio al momento de la interrupción o falla de operación del equipamiento. Valor = 4 un impacto alto al momento de la interrupción o falla de operación del equipamiento. Valor = 5 representa un impacto catastrófico al momento de la interrupción o falla del equipamiento.

Tabla 8 Escala de impacto de aplicaciones del MDMQ

Valor	Escala de Impacto
1	Bajo
2	Moderado
3	Medio
4	Alto
5	Catastrófico

4.1.8.12 Calificación de la probabilidad de falla del equipamiento del data center MDMQ

Se ha manejado una escala del 1 al 4 la priorización del impacto donde valor = 1 representa la probabilidad baja de producirse la falla del equipamiento. Valor = 2 representa la probabilidad media de producirse la falla del equipamiento. Valor = 3 una probabilidad alta de producirse la falla del equipamiento. Valor = 4 una probabilidad catastrófica de producirse la falla del equipamiento.

Tabla 9 Escala de probabilidad de falla del equipamiento.

Valor	Escala de Probabilidad
1	Bajo
2	Medio
3	Alto
4	Catastrófico

4.1.8.13 Priorización del riesgo

Para establecer el riesgo se maneja tres escalas para la priorización del riesgo donde: Riesgo 1 > = 5 son riesgos bajos, cuando un equipo fallara. Riesgo 6 > = 10 riesgos medios, cuando un equipo fallara. Riesgo 11 > = 15 altos, cuando un equipo fallara. Riesgo 16 > = 20 Catastróficos, cuando un equipo fallara.

4.1.8.14 Tabla de riesgo

Se construye dicha tabla tomando la relación entre riesgo e impacto, en el eje vertical se ubica el impacto y el eje horizontal el riesgo y en cada cuadrante según la escala se encuentran los equipos que se encuentran en el data center del MDMQ.

4.1.8.15 Listado del equipamiento del data center

Tabla 10 Listado de Servicios de Equipamiento del Data Center

Escala de Impacto	Escala de Probabilidad
1 Bajo	1 Bajo
2 Moderado	2 Medio
3 Medio	3 Alto
4 Alto	4 Catastrófico
5 Catastrófico	

Equipamiento Data Center	Código	Impacto	Probabilidad	Riesgo
Librería de Respaldos	L1	5	2	10
Aire Acondicionado	L2	4	2	8
Generador Eléctrico	L3	4	2	8
Panel de incendios	L4	4	2	8
PDU	L5	5	1	5
Tanque de suspensión de Incendios	L6	4	1	4
Tablero de Distribución Eléctrico	L7	3	1	3
Sensor de Temperatura	L8	3	1	3
Lector de Huellas Digitales	L9	3	1	3
Sistema de Alarmas	L10	2	1	2
Uninterruptible Power Supply (UPS)	L11	2	1	2
Sensor de Humo	L12	2	1	2
Sistema de Monitoreo de Cámaras	L13	2	1	2
Sistema de Iluminación	L14	2	1	2
Sistemas de Monitoreo y Control de IP	L15	2	1	2
Sirena	L16	1	1	1
Botón de Pánico	L17	1	1	1
Detector de Movimiento	L18	1	1	1
Piso Falso	L19	1	1	1
Rack	L20	1	1	1

4.1.8.16 Tabla de intervalos de riesgos equipamiento de Data Center

Se presenta en la siguiente tabla de riesgos de falla sobre los equipos que se encuentran en el data center

Tabla 11 Intervalos de Riesgos para Equipamiento de Data Center

Tabla de Riesgos	
Riesgo 1 > = 5	Bajo
Riesgo 6 > = 10	Medio
Riesgo 11 > = 15	Alto
Riesgo 11 > = 15	Catastróficos

4.1.8.17 Tabla de priorización de equipamiento del Data Center según riegos

En la siguiente tabla indica los equipos del data center calificados con riesgos medio, alto o catastrófico, descartando los de riesgo bajo.

Tabla 12 Listado priorizados de Equipamiento del Data Center según su riesgo.

Equipamiento Data Center	Código	Impacto	Probabilidad	Riesgo
Librería de Respaldos	L1	5	2	10
Aire Acondicionado	L2	4	2	8
Generador Eléctrico	L3	4	2	8
Panel de incendios	L4	4	2	8

4.1.8.18 Tabla de riesgos del equipamiento Data Center por impacto y Prioridad

En la siguiente tabla de riesgos, se conforma ubicando los códigos de los equipos en los cuadrantes correspondientes según su impacto y probabilidad.

Tabla 13 Impacto vs Probabilidad del Equipamiento del Data Center del MDMQ

	5 catastrófico	L5	L1		
	4 alto	L6	L2,L3,L4		
Impacto	3 medio	L7.L8,L9			
	2 moderado	L10,..,L15			
	1 bajo	L16,..,L20			
		1 bajo	2 medio	3	4

			alto	Catastrófico
		Probabilidad		

4.1.8.19 Listado de servicios de terceros

Está tabla está conformada de columna 1 conformada 12 principales servicios de terceros que son contratados MDMQ. Columna 2 Código que representa al servicio de terceros se representa con la letra s y un número consecutivo. Columna 3 impacto que se califica si un servicio deje de funcionar o presente aluna falla el cual no permita su correcto funcionamiento. Columna 4 probabilidad que significa que tan posible es que se presente la falla del servicio. Columna 5 riesgo que se obtendrá de la multiplicación del impacto por la probabilidad.

4.1.8.20 Calificación del impacto

Se ha manejado una escala del 1 al 5 para la calificación al impacto a relación cuando un servicio deja de funcionar. Donde valor = 1 representa un impacto bajo al momento de la interrupción o falla del servicio. Valor = 2 representa un impacto moderado al momento de la interrupción o falla del servicio. Valor = 3 es un impacto medio al momento de la interrupción o falla de operación del servicio. Valor = 4 un impacto alto al momento de la interrupción o falla de operación del servicio. Valor = 5 representa un impacto catastrófico al momento de la interrupción o falla del servicio.

Tabla 14 Escala de impacto sobre los servicios de terceros

Valor	Escala de Impacto
1	Bajo
2	Moderado
3	Medio
4	Alto
5	Catastrófico

4.1.8.21 Calificación de la probabilidad

Se maneja una escala del 1 al 4 la priorización del impacto donde valor = 1 representa la probabilidad baja de producirse la falla del servicio. Valor = 2 representa la probabilidad media de producirse la falla del servicio. Valor = 3 una probabilidad alta de producirse la falla del servicio. Valor = 4 una probabilidad catastrófica de producirse la falla del servicio.

Tabla 15 de escala de probabilidad de falla del servicio de terceros

Valor	Escala de Probabilidad
1	Bajo
2	Medio
3	Alto
4	Catastrófico

4.1.8.22 Priorización del riesgo

Para establecer el riesgo se maneja tres escalas para la priorización del riesgo donde riesgo 1 > = 5 son riesgos bajos, cuando un servicio fallara. Riesgo 6 > = 10 riesgos medios, cuando un servicio fallara. Riesgo 11 > = 15 altos, cuando un servicio fallara. Riesgo 16 > = 20 Catastróficos, cuando un servicio fallara.

4.1.8.23 Listado de servicio de terceros

Tabla 16 Servicios Terceros

Escala de Impacto	Escala de Probabilidad
1 Bajo	1 Bajo
2 Moderado	2 Medio
3 Medio	3 Alto
4 Alto	4 Catastrófico
5 Catastrófico	

Servicios Terceros	Código	Impacto	Probabilidad	Riesgo
Enlaces WAN	S1	5	2	10
Internet CNT	S2	4	2	8
Internet Redundancia Telconet	S3	4	2	8
Licenciamiento	S4	4	2	8
Soporte Equipos	S5	3	2	6
Energía Eléctrica	S6	5	1	5
Enlace Band Red	S7	5	1	5
Mantenimiento Preventivo de hardware	S8	2	2	4
Soporte Aplicaciones	S9	2	2	4
Telefonía	S10	3	1	3
Host y Honsting	S11	3	1	3
Desarrollo Externo de Aplicaciones	S12	3	1	3

4.1.8.24 Tabla de riesgos de los servicios de terceros

Se presenta en la siguiente tabla de riesgos al fallar un servicio.

Tabla 17 Intervalos de Riesgos para Servicios de terceros

Tabla de Riesgos	
Riesgo 1 > = 5	Bajo
Riesgo 6 > = 10	Medio
Riesgo 11 > = 15	Alto
Riesgo 11 > = 15	Catastróficos

4.1.8.25 Tabla de priorización de servicios de terceros

En la siguiente tabla indica los servicios calificados con riesgos medio, alto o catastrófico, descartando los de riesgo bajo.

Tabla 18 Listado priorizados de Servicios de Terceros

Servicios Terceros	Código	Impacto	Probabilidad	Riesgo
Enlaces WAN	S1	5	2	10
Internet CNT	S2	4	2	8
Internet Redundancia Telconet	S3	4	2	8
Licenciamiento	S4	4	2	8

4.1.8.26 Tabla de riesgos de servicios de terceros por impacto y prioridad

En la siguiente tabla de riesgos, se conforma ubicando los códigos de los servicios en los cuadrantes correspondientes según su impacto y probabilidad.

Tabla 19 Impacto vs Probabilidad de Servicios de Terceros.

	5 catastrófico	S6,S7	S1		
	4 alto		S2,S3,S4		
Impacto	3 medio	S10,S10,S12	S5		
	2 moderado		S8,S9		
	1 bajo	S6,S7	S1		
		1 bajo	2 medio	3 alto	4 catastrófico

Probabilidad

4.1.8.27 Tabla de equipos de telecomunicaciones y redes

Esta tabla está conformada de Columna 1 conformada 22 elementos principales de equipos de telecomunicaciones y redes. Columna 2 Código que representa a los equipos de telecomunicación y redes representados por la letra R y un número consecutivo. Columna 3 número aproximado de usuarios que se verían afectados al dejar de funcionar los equipos de telecomunicación y redes. Columna 4 impacto que se califica a los equipos de telecomunicación y redes cuando este deje de funcionar o presente aluna falla el cual no permita su correcto funcionamiento. Columna 5 probabilidad que significa que tan posible es que se presente la falla de los equipos de telecomunicación y redes. Columna 6 riesgo que se obtendrá de la multiplicación del impacto por la probabilidad

4.1.8.28 Calificación del impacto

Se maneja una escala del 1 al 5 para la calificación al impacto a los equipos de telecomunicación y redes donde valor = 1 representa un impacto bajo al momento de la interrupción o falla de los equipos de telecomunicación y redes.

Valor = 2 representa un impacto moderado al momento de la interrupción o falla de operación de los equipos de telecomunicación y redes. Valor=3 es un impacto medio al momento de la interrupción o falla de operación de los equipos de telecomunicación y redes. Valor = 4 un impacto alto al momento de la interrupción o falla de operación de los equipos de telecomunicación y redes. Valor = 5representa un impacto catastrófico al momento de la interrupción o falla de operación de los equipos de telecomunicación y redes

Tabla 20 de escala de impacto de los equipos de telecomunicación y redes

Valor	Escala de Impacto
1	Bajo
2	Moderado
3	Medio
4	Alto
5	Catastrófico

4.1.8.29 Calificación de la probabilidad

Se ha manejado una escala del 1 al 4 la priorización del impacto donde valor = 1 representa la probabilidad baja de producirse la falla de los equipos de telecomunicación y redes. Valor = 2 representa la probabilidad media de producirse la falla de los equipos de telecomunicación y redes. Valor = 3 una probabilidad alta de producirse la falla de los equipos de telecomunicación y redes. Valor = 4 una probabilidad catastrófica de producirse la falla de los equipos de telecomunicación y redes.

Tabla 21 de escala de probabilidad de falla de los equipos de telecomunicación y redes

Valor	Escala de Probabilidad
1	Bajo
2	Medio
3	Alto
4	Catastrófico

4.1.8.30 Priorización del riesgo

Para establecer el riesgo se maneja tres escalas para la priorización del riesgo donde riesgo 1 > = 5 son riesgos bajos, cuando un equipos de telecomunicación y redes fallara. Riesgo 6 > = 10 riesgos medios, cuando un equipos de telecomunicación y redes fallara. Riesgo 11 > = 15 altos, cuando un equipos de telecomunicación y redes fallara. Riesgo 16 > = 20 Catastróficos, cuando un equipos de telecomunicación y redes fallara.

4.1.8.31 Tabla de riesgo

Se construye dicha tabla tomando la relación entre riesgo e impacto, en el eje vertical se ubica el impacto y el eje horizontal el riesgo y en cada cuadrante según la escala se encuentran las aplicaciones que posee la MDMQ.

4.1.8.32 Listado de equipos de telecomunicaciones y redes

Tabla 22 de listado de equipos de telecomunicaciones y redes.

Escala de Impacto	Escala de Probabilidad
1 Bajo	1 Bajo
2 Moderado	2 Medio
3 Medio	3 Alto
4 Alto	4 Catastrófico
5 Catastrófico	

Equipos de Telecomunicaciones y redes	Código	Número de Usuarios	Impacto	Probabilidad	Riesgo
Infraestructura					
Switch core	R1	8000	5	1	5
Switch capa 2	R2	5000	2	2	4
Switch capa 3	R3	5000	4	1	4
Routes	R4	5000	4	1	4
Ons	R5	40	3	2	6
Equipos de seguridad					
Firewall	R6	5000	4	1	4

Continúa…

Equipo de control de acceso a la web y Manejo de Vpns	R7	8000	4	1	4
Ips	R8	8000	2	2	4
Access control server (ACS)	R9	2000	3	1	3
Balanceadores de carga	R10	700	3	1	3
Equipos de telefonía					
Media gateway	R11	3000	4	1	4
System Manager	R12	3000	3	1	3
Comunication Manager	R13	3000	4	1	4
Session Manager	R14	3000	3	1	3
Sesion border controler	R15	1500	2	2	4
vioce portal	R16	1000	2	1	2
Modular messaging	R17	8000	1	1	1
Tarifador	R18	8000	2	2	4
Application Enablement Services (Aes)	R19	2000	1	1	1
Redes Inalámbricas					
Controladores wireless	R20	2000	5	1	5
Wimax Controlador	R21	3000	5	2	10
Wimax RadioBases	R22	3000	3	2	6

4.1.8.33 Listado priorizados de los equipos de telecomunicación y redes según su riesgo.

En la siguiente tabla indica los equipos de telecomunicaciones y redes calificados con riesgos medio, alto o catastrófico, descartando los de riesgo bajo.

Tabla 23 de listado priorizado de equipos de telecomunicaciones y redes.

Equipos de Telecomunicaciones y redes	Código	Número de Usuarios	Impacto	Probabilidad	Riesgo
Wimax Controlador	R21	3000	5	2	10
Wimax RadioBases	R22	3000	3	2	6
Ons	R5	40	3	2	6

4.1.9.34 Tabla de riesgos de los equipamiento telecomunicaciones y equipos de redes

Se presenta la tabla de riesgos de los equipos de telecomunicaciones y redes.

Tabla 24 Impacto vs Probabilidad de los equipos telecomunicaciones y redes.

Tabla de Riesgos	
Riesgo 1 > = 5	Bajo
Riesgo 6 > = 10	Medio
Riesgo 11 > = 15	Alto
Riesgo 11 > = 15	Catastróficos

4.1.8.35 Tabla de riesgos del equipamiento telecomunicaciones y equipos de redes por impacto y prioridad.

El diagrama de la tabla de riesgos, se conforma ubicando los códigos de los equipos de telecomunicaciones y redes en los cuadrantes correspondientes según su impacto y probabilidad.

Tabla 25 Impacto vs Probabilidad de Equipamiento Telecomunicaciones y Equipos de Redes

Impacto	5 Catastrófico	R1,R20	R21		
	4 Alto	R3,R4,R6,R7, R11,R13			
	3 Medio	R9,R10,R12, R14	R5,R22		
	2 Moderado	R16	R2,R8,R15, R18		
	1 Bajo	R17			

Continúa…

	1 Bajo	2 Medio	3 alto	4 Catastrófico
		Probabilidad		

4.1.8.36 Tabla de riesgos de seguridad sobre el personal que labora en el data center

Está tabla está conformada de columna 1 conformada 8 principales riesgos de seguridad que se puede presentar sobre el personal que labora en el data center. Columna 2 código que representa los riesgos que se puede presentar sobre el personal que labora en el data center. Columna 3 impacto que se califica si un persona que labora en el data center divulga datos confidenciales. Columna 4 probabilidad que significa que tan posible que el personal divulgue información sensible. Columna 5 riesgo que se obtendrá de la multiplicación del impacto por la probabilidad.

4.1.8.37 Calificación del impacto

Se ha manejado una escala del 1 al 5 para la calificación al impacto a relación cuando una persona que labora en el área del data center divulga información confidencial o sensible donde valor = 1 representa un impacto bajo al momento que el personal entrega información pública. Valor = 2 representa un impacto moderado al momento el personal entrega información no sensible. Valor=3 es un impacto medio al momento el personal entrega información restringida. Valor = 4 un impacto alto al momento el personal entrega información sensible. Valor = 5representa un impacto catastrófico el personal entrega información crítica.

Tabla 26 de escala de impacto del personal a divulgar información

Valor	Escala de Impacto
1	Bajo
2	Moderado
3	Medio
4	Alto
5	Catastrófico

4.1.8.38 Calificación de la probabilidad

Se maneja una escala del 1 al 4 la priorización del impacto donde valor = 1 representa la probabilidad baja a la divulgación de información crítica o sensible. Valor = 2 representa la probabilidad media a la divulgación de información crítica o sensible. Valor = 3 una probabilidad alta a la divulgación de información crítica o sensible. Valor = 4 una probabilidad catastrófica a la divulgación de información crítica o sensible.

Tabla 27 de escala de probabilidad de entrega de información por el personal.

Valor	Escala de Probabilidad
1	Bajo
2	Medio
3	Alto
4	Catastrófico

4.1.8.39 Priorización del riesgo

Para establecer el riesgo se maneja tres escalas para la priorización del riesgo donde riesgo 1 > = 5 son riesgos bajos. Riesgo 6 > = 10 riesgos medios. Riesgo 11 > = 15 altos. Riesgo 16 > = 20 Catastróficos.

4.1.8.40 Listado de riesgos de seguridad por parte del personal del data center

Tabla 28 Riesgos de seguridad que se puede presentar por el personal del data center

Escala de Impacto	Escala de Probabilidad
1 Bajo	1 Bajo
2 Moderado	2 Medio
3 Medio	3 Alto
4 Alto	4 Catastrófico
5 Catastrófico	

Riesgo sobre el personal	Código	Impacto	Probabilidad	Riesgo
Ingeniería Social	P1	5	2	10
Robo de Información crítica o sensible	P2	5	1	5
Alteración de datos críticos o sensibles por el personal	P3	5	1	5
Extorción al personal Clave	P4	4	1	4
Secuestro al personal clave	P5	4	1	4
No cumplimiento del cumplimiento del compromiso de confidencialidad	P6	4	1	4
Espionaje del Personal	P7	4	1	4
Utilización de código malicioso puertas traseras por los desarrolladores de las aplicaciones	P8	4	1	4

4.1.8.41 Tabla de riesgos del personal

Se presenta en la siguiente tabla de riesgos de seguridad por parte del personal

Tabla 29 Intervalos de Riesgos del personal

Tabla de Riesgos	

Riesgo 1 > = 5	Bajo
Riesgo 6 > = 10	Medio
Riesgo 11 > = 15	Alto
Riesgo 11 > = 15	Catastróficos

4.1.8.42 Tabla de priorización de seguridad sobre el personal según sus riesgos

En la siguiente matriz indica los riesgos que puede presentarse al personal calificados con riesgos medio, alto o catastrófico, descartando los de riesgo bajo.

Tabla 30 Listado priorizados de los Riesgos que se puede presentar por el personal

Riesgo sobre el personal	Código	Impacto	Probabilidad	Riesgo
Ingeniería Social	P1	5	2	10

4.1.8.43 Tabla de riesgos del personal por impacto y prioridad

En la siguiente tabla de riesgos, se conforma ubicando los códigos de los servicios en los cuadrantes correspondientes según su impacto y probabilidad.

Tabla 31 Impacto vs Probabilidad del Personal

	5 catastrófico	P2,P3	P1		
	4 alto	P4,…,P8			
Impacto	3 medio				
	2 moderado				
	1 bajo				
		1 bajo	2 moderado	3 alto	4 Catastrófico
			Probabilidad		

4.1.8.44 Tabla de equipos enclouser

Esta primera matriz está conformada de Columna 1 conformada 18principales equipos enclouser donde se alojan servidores baldes. Columna 2 Código que representa a los equipos representados con las letras SRV y un consecutivo numérico. Columna 3 Impacto que se califica a los equipos cuando este deje de funcionar o presente alguna falla el cual no permita su correcto funcionamiento. Columna 4 probabilidades que significa que tan posible es que se

presente la falla de los equipos Columna 5: riesgo que se obtendrá de la multiplicación del impacto por la probabilidad

4.1.8.45 Calificación del impacto

Se ha manejado una escala del 1 al 5 para la calificación al impacto a las aplicaciones cuando esta deja funcionar o tiene una interrupción donde valor = 1 representa un impacto bajo al momento de la interrupción o falla de operación de los equipos. Valor = 2 representa un impacto moderado al momento de la interrupción o falla de operación de los equipos. Valor=3 es un impacto medio al momento de la interrupción o falla de operación de los equipos. Valor = 4 un impacto alto al momento de la interrupción o falla de operación de los equipos. Valor = 5 representa un impacto catastrófico al momento de la interrupción o falla de operación de los equipos.

Tabla 32 de escala de impacto de equipos de encloser.

Valor	Escala de Impacto
1	Bajo
2	Moderado
3	Medio
4	Alto
5	Catastrófico

4.1.8.46 Calificación de la probabilidad

Se ha manejado una escala del 1 al 4 la priorización del impacto donde valor = 1 representa la probabilidad baja de producirse la falla de los equipos. Valor = 2 representa la probabilidad media de producirse la falla de los equipos. Valor = 3 una probabilidad alta de producirse la falla de los equipos. Valor = 4 una probabilidad catastrófica de producirse la falla de los equipos.

Tabla 33 de escala de probabilidad de falla de los equipos

Valor	Escala de Probabilidad
1	Bajo
2	Medio
3	Alto
4	Catastrófico

4.1.8.47 Priorización del riesgo

Para establecer el riesgo se maneja tres escalas para la priorización del riesgo donde riesgo 1 > = 5 son riesgos bajos, cuando un equipo fallará. Riesgo 6 > = 10 riesgos medios, cuando un equipo fallará. Riesgo 11 > = 15 altos, cuando un equipo fallará. Riesgo 16 > = 20 Catastróficos, cuando un equipo fallará.

4.1.8.48 Matriz de riesgo

La tabla se conforma con la relación entre riesgo e impacto, en el eje vertical se ubica el impacto y el eje horizontal el riesgo y en cada cuadrante según la escala se encuentran los equipos.

4.1.8.49 Listado de equipos del MDMQ

Tabla 34 Equipamiento de Servidores

Escala de Impacto	Escala de Probabilidad
1 Bajo	1 Bajo
2 Moderado	2 Medio
3 Medio	3 Alto
4 Alto	4 Catastrófico
5 Catastrófico	

Equipamiento Servidores	Código	Impacto	Probabilidad	Riesgo
Encluser IBM CHASIS E	srv01	5	2	10
Encluser Hp C3000 (Bomberos) físico	srv02	5	2	10
STORAGE DS-3400	srv03	5	2	10
STORAGE P6500(1)	srv04	5	2	10
STORAGE P6500(2) tipo 4 (Educación)	srv05	5	2	10
STORAGE P2000(1)	srv06	5	2	10
Encluser IBM CHASIS H	srv07	4	2	8
Encluser Hp C7000 tipo 2 (sirecq)	srv08	4	2	8

Continúa…

Encluser Hp C7000 tipo 2 (sirecq)	srv09	4	2	8
Encluser Hp C7000 tipo 3 (Enduc)	srv10	4	2	8
Encluser Hp C7000 tipo 3 (Enduc)	srv11	4	2	8
Encluser Hp C7000	srv12	4	2	8
Librería MSL 4048	srv13	4	1	4
Encluser Hp C7000 Tipo 1	srv14	3	1	3
blades RX8640	srv15	3	1	3
blades RX8640	srv16	3	1	3
storage EVA8100	srv17	3	1	3
Librería MSL 6060	srv18	3	1	3

4.1.8.50 Tabla de priorización de equipamiento de servidores según riegos

En la siguiente tabla indica los equipos que fueron calificados con riesgos medio, alto o catastrófico, descartando los de riesgo bajo.

Tabla 35 Listado priorizados de Equipamiento de Servidores

Equipamiento Servidores	código	Impacto	Probabilidad	Riesgo
Encluser IBM CHASIS E	srv01	5	2	10
Encluser Hp C3000 (Bomberos) físico	srv02	5	2	10
STORAGE DS-3400	srv03	5	2	10
STORAGE P6500(1)	srv04	5	2	10
STORAGE P6500(2) tipo 4 (Educación)	srv05	5	2	10
STORAGE P2000(1)	srv06	5	2	10
Encluser IBM CHASIS H	srv07	4	2	8
Encluser Hp C7000 tipo 2 (sirecq)	srv08	4	2	8
Encluser Hp C7000 tipo 2 (sirecq)	srv09	4	2	8
Encluser Hp C7000 tipo 3 (Enduc)	srv10	4	2	8
Encluser Hp C7000 tipo 3 (Enduc)	srv11	4	2	8
Encluser Hp C7000	srv12	4	2	8

4.1.8.51 Tabla de riesgos de equipos de servidores

Se presenta la tabla de riesgos en relación de los equipos

Tabla 36 Tabla de riesgos de equipos de servidores

Tabla de Riesgos	
Riesgo 1 > = 5	Bajo
Riesgo 6 > = 10	Medio
Riesgo 11 > = 15	Alto
Riesgo 11 > = 15	Catastróficos

4.1.8.52 Tabla de riesgos de equipamiento de servidores por impacto y prioridad

El diagrama de la tabla de riesgos, se conforma ubicando los códigos de los equipos en los cuadrantes correspondientes según su impacto y probabilidad.

Tabla 37 Impacto vs Probabilidad de Equipamiento de Servidores

	5 catastrófico		Srv02,..srv06	Srv01	
	4 alto	srv13	srv07,..,srv012		
Impacto	3 medio	srv14,…srv18			
	2 moderado				
	1 bajo				
		1 bajo	2 medio	3 alto	4 Catastrófico
			Probabilidad		

4.1.9 Evaluación basada en riesgos bajo la norma ISO/IEC 27001:2005 / Sistema de Gestión de la Seguridad de la Información (SGSI)

4.1.9.1 Análisis de riesgo

Se realizó una calificación de los riesgos que va hacer evaluados en base a los procesos del SGSI, que posee norma ISO/IEC 27001:2005basado en sus cláusulas de la 4 – 8.

4.1.9.2 Selección de procesos y escenarios a ser evaluados

La tabla de riesgos y controles de la Norma ISO/IEC 27001:2005 SGSI consta de los siguientes campos:

- **Cláusulas del SGSI**.- Describe las cláusulas que establece el SGSI en forma general.
- **Fuente de consulta**.- Define el responsable del departamento quien aporto para la calificación del riesgo.
- **Técnica de campo**.- Describe la técnica de Investigación.
- **Documentos de referencia.-** Describe los documentos de sustento.
- **Cumplimiento.-** Detalla si cumple o no las cláusulas.
- **Hallazgos**.- Detallas los hallazgos encontrados de las cláusulas del SGSI.
- **Recomendaciones**.- Detallas las recomendaciones de los hallazgos encontrados.

Tabla 38 Tabla de Calificación de Controles norma ISO/IEC 27001:2005 / SGSI

ISO/IEC 27001:2005 / SGSI

4.1.10 Evaluación basada en riesgos tabla Anexo A norma ISO/IEC 27001:2005/ ISO/IEC 27002:2005 objetivos de control y controles

4.1.10.1 Análisis de riesgo

Se realizó una calificación de los riesgos que va hacer evaluados en base a los controles que posee norma tabla Anexo A norma ISO/IEC 27001:2005 / ISO/IEC 27002:2005, este criterio fue tomado en conjuntos con las autoridades y el personal clave de la DMI, quienes con su vasto conocimiento llegaron a una clasificación de riesgos, determinando una escala con valores alto, medio y bajo según el grado de criticidad.

Los riesgos con calificación baja solo serán descritos mas no serán tomados en cuenta para la evaluación de los controles de la norma tabla Anexo A norma ISO/IEC 27001:2005 / ISO/IEC 27002:2005, los controles que estén dentro de los parámetros entre medios y altos serán tomados en cuenta para la evaluación de su cumplimiento.

4.1.10.2 Selección de procesos y escenarios a ser evaluados

La tabla de riesgos y controles de la norma tabla Anexo A norma ISO/IEC 27001:2005 / ISO/IEC 27002:2005consta de los siguientes campos:

- **Objetivo del control**.- Contiene los objetivos del control descrito en forma general.
- **Fuente de consulta**.- Define el responsable del departamento quien aporto para la calificación del riesgo.
- **Técnica de campo**.- Describe la técnica de Investigación.
- **Documentos de referencia.-** Describe los documentos de sustento.

- **Cumplimiento.-** Detalla si cumple o no las cláusulas.
- **Riesgo**.- Clasifica entre catastrófico, alto, medio y bajo.
- **Hallazgos**.- Detallas los hallazgos encontrados en los controles de la norma tabla Anexo A norma ISO/IEC 27001:2005 / ISO/IEC 27002:2005.
- **Recomendaciones**.- Detallas las recomendaciones de los hallazgos encontrados.

Tabla 39 Tabla de Calificación de Controles de tabla Anexo A norma ISO/IEC 27001:2005 / ISO/IEC 27002:2005 objetivos de control y controles

Capítulo V

5.1 Informe final

5.1.1 Informe Detallado “objetivo del informe, alcance, metodología, y los resultados o hallazgos”.

5.1.1.1 Informe de Auditoria

5.1.1.1.1 Objetivo del informe

La verificación del cumplimiento de los controles de seguridad que posee el Data Center la Dirección de Informática versus los controles y objetivos de control de las normas ISO 27001:2005 e ISO 27002:2005.

5.1.1.1.2 Alcance del informe

El informe conlleva a una validación de los controles que posee actualmente el Data Center de la Dirección de Informática, validándolo con las normas ISO 27001:2005 e ISO 27002:2005.

Este informe se lo socializara a las autoridades de la Dirección de Informática para el análisis de los hallazgos encontrados y las recomendaciones que se sugiere y sobre esto puedan tomar decisiones al respecto.

5.1.1.1.3 Metodología utilizada: auditoria basada en riesgos

Para el desarrollo del documento se obtuvo la información mediante encuestas y entrevistas al personal técnico informático que labora en la Dirección

Metropolitana de Informática, además de la observación de los procesos de seguridad manejados.

A continuación se describe los controles de las normas ISO 27001:2005 e ISO 27002:2005, los hallazgos y las recomendaciones sugeridas

5.1.1.1.4 Hallazgos

5.1.1.1.4.1 Hallazgos de la matriz de controladores ISO 27001:2005SGSI

La dirección de informática no cuenta con un sistema de gestión de la seguridad de la información (SGSI), solo con algunos controles de esta matriz que se los ha implementados empíricamente, por lo que no se puede auditar a detalle todo los controles. Se describe a continuación los controles que parcialmente cumplen.

5.1.1.1.4.1.1 Establecimiento del SGSI

Inicio del Proyecto

Definición del SGSI

Análisis de Riesgos

Gestión de Riesgos

Hallazgo

No cuenta con políticas y procedimientos del SGSI

Recomendación

Creación de procedimientos para el SGSI

5.1.1.1.4.1.2 Implantación y Operación

Implantación del SGSI

Hallazgo

No cuenta con políticas y procedimientos del SGCI

Recomendación

Creación de procedimientos para el SGCI

5.1.1.1.4.1.3 Monitorización y Revisión

Monitorización del SGSI

Revisión del SGSI

Hallazgo

No cuenta con políticas y procedimientos del SGCI

Recomendación

Creación de procedimientos para el SGCI

5.1.1.1.4.1.4 Mantenimiento y Mejora

Mantenimiento del SGSI

Mejora Continua

Hallazgo

No cuenta con políticas y procedimientos del SGCI

Recomendación

Creación de procedimientos para el SGCI

5.1.1.1.4.2 HALLAZGOS DE LA MATRIZ DE CONTROLADORES ISO27002:2005

5.1.1.1.4.2.1 Control de la Norma (A.5.1.1)

La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.

Hallazgo

Las Políticas se encuentra publicado y disponibles en el sitio del portal de la intranet del Municipio del Distrito Metropolitano de Quito, el cual tiene acceso todos los usuarios por tal motivo cumple el control

Recomendación

Se pueden difundir las políticas por otros medios de comunicación como son la página oficial del MDMQ y deben ser socializadas a los empleados mediante charlas de concientización.

5.1.1.1.4.2.2 Revisión de la política de seguridad de la información (A.5.1.2)

La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad."

Hallazgo

La Políticas fueron elaboradas revisadas y autorizadas en el año 2011, desde aquella fecha no se realizado ninguna actualización al documento de políticas de gestión de tecnológicas

Recomendación

Se debería establecer un comité de seguridad para mantener y actualizar y socializar el documento de políticas de gestión de tecnología, este proceso se debería realizar al menos una vez al año.

5.1.1.1.4.2.3 Coordinación de la seguridad de información (A.6.1.2)

Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.

Hallazgo

No existe representante, funciones y roles de las áreas sensibles de tecnología. Cada área de la DMI aplica criterios seguridad de forma independiente de manera que cree, la seguridad de la información. No existe ningún procedimiento formal

Recomendación

Se debe mantener un comité de seguridad formal, con directrices, procesos y roles claros los cuales establezcan la seguridad de la información.

5.1.1.1.4.2.4 Asignación de responsabilidades de la seguridad de la información (A.6.1.3)

Se deben definir claramente las responsabilidades de la seguridad de la información.

Hallazgo

Existe un único documento llamado Políticas de Gestión de Información donde se establecen las responsabilidades de políticas de seguridad, las cuales son muy genéricas.

Recomendación

La información es el activo más importante de la institución, por lo que se recomienda se establezca responsabilidades bien definidas sobre la seguridad de la información, en las áreas críticas.

5.1.1.1.4.2.5 Revisión independiente de la seguridad de la información (6.1.8)

El enfoque de la organización para manejar la seguridad de la información y su implementación(es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.

Hallazgo

Al momento los procesos, objetivos, controles y procedimientos de seguridad no son actualizados a intervalos de tiempo. Los documentos consultados como Políticas de gestión de información es un documento del año del 2011 que no se actualizado desde aquella época.

Recomendación

Los documentos concernientes a objetivos, controles, procedimientos para seguridad deben establecerse un periodo para realizar las actualizaciones a dichos documentos

5.1.1.1.4.2.6 Tratamiento de la seguridad en contratos con terceras personas (6.2.3)

Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.

Hallazgo

Cumple con el control satisfactoriamente, según el documento de solicitud de permisos de accesos que se maneja en el DMI. Porque solo permiten el acceso únicamente al área que corresponde.

Recomendación

Se recomienda poseer un departamento de seguridad el cual se dedique a verificar cumplimiento de políticas y normas de seguridad las cuales son imprescindibles para el buen resguardo de la información.

5.1.1.1.4.2.7 Lineamientos de clasificación (7.2.1)

La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.

Hallazgo

Según los documentos de servicios el cual identifica los recursos que se manejan cada proceso. No se tiene definida claramente el tipo de información que se posee en el MDMQ como la crítica, sensible, confidencial, y publica

Recomendación

Los dueños de la información deben definir el tipo (crítica, sensible, confidencial y pública).

5.1.1.1.4.2.8 Etiquetado y manejo de la información (7.2.2)

Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

Hallazgo

En los manuales de servicios no se tiene desarrollado, ni implementado un procedimiento para etiquetar el tipo de información

Recomendación

Crear procedimientos para que daca dueño pueda etiquetar el tipo de información que se maneja en el MDMQ

5.1.1.1.4.2.9 Roles y responsabilidades (8.1.1)

Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.

Hallazgo

Se ha verificado los contratos que se realiza con diferentes entes pero no se establecen los roles y responsabilidades de la seguridad para los contratistas y terceros en con concordancia políticas de seguridad que posee el Municipio de distrito Metropolitano de Quito

Recomendación

Establecer clase responsabilidades y los roles de seguridad cuando un contratista o tercero va a trabajar en el MDMQ además la política de seguridad debe actualizarse para mejorar los alcances de esos entes.

5.1.1.1.4.2.10 Capacitación y educación en seguridad de la información (8.2.2)

Todos los empleados de la organización y cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

Hallazgos

Se ha revisado los planes de capacitación que anual mente se debe realizar, no existe capacitación sobre las políticas y procedimientos organizaciones para el personal, contratistas o terceros. Los documentos de políticas se encuentran en la intranet de la organización.

Recomendaciones

Al menos una vez al año se debe capacitar al personal, contratistas o terceros sobre los temas de políticas y procedimientos organizaciones.

5.1.1.1.4.2.11 Eliminación de derechos de acceso (8.3.3)

Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.

Hallazgos

Se encontró que al momento que se da por terminado el contrato con empleados, contratistas y terceros los accesos a la información no son retirados o

eliminados inmediatamente, en consecuencia otro personal que conozca los accesos puede cometer algún tipo de alteración intencionada esto fue verificado con los técnicos que manejan los sistemas.

Recomendaciones

El área que verifica en las terminaciones de contratos. Debería enviar una notificación inmediatamente a los responsables departamentales indicando que se retire los accesos.

5.1.1.1.4.2.12 Trabajo en áreas seguras (9.1.5)

Se debe aplicar seguridad al equipo fuera-del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

Hallazgos

El ingreso al data center existen protecciones físicas para todo el personal que ingresa como son puertas, y accesos con tarjetas de identificación y lectores biométricos. No existe un documento donde se encuentren descritos lineamientos de trabajo.

Recomendaciones

Crear un documento donde se establezca los lineamientos sobre los trabajos que se pueden realizar en el data center tanto para el personal como para proveedores

5.1.1.1.4.2.13 Seguridad del equipo fuera-del local (9.2.5)

Se debe aplicar seguridad al equipo fuera-del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

Hallazgos

Cuando un equipo sale de la organización, no se ejecuta las mismas políticas que al estar el interior esto fue verificado con equipos que salieron de la red municipal no mantuvieron las políticas, tampoco actualizaciones a las soluciones de seguridad de los equipos.

Recomendaciones

Todo equipo que pertenezca a la organización y tenga que salir debe contar con las mismas protecciones como que estuviera dentro de esta.

5.1.1.1.4.2.14 Eliminación seguro o re-uso del equipo (9.2.6)

Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.

Hallazgos

La información que poseen, los medios de procesamiento de información que se encuentran en el data center no son eliminados permanente. Cuando se lo va a dar de baja por cumplir su vida útil o al ser reutilizado en otra dependencia Se validó con el administrador de infraestructura que los equipos que cumplen su

tiempo de vida son únicamente dados de baja para su envió a bodega o de entrega a otra dependencia para su reutilización.

Recomendaciones

Tener como política la eliminación definitiva de la información que almacena de todos los medios de procesamiento de información que posee el data center. Antes de ser eliminados y ser reutilizados.

5.1.1.1.4.2.15 Procedimientos de operación documentados (A.10.1.1)

Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

Hallazgos

No existe la suficiente documentación y procedimientos que se generan para la operación tanto de las aplicaciones, servidores, equipamiento del data center, equipos de red y telecomunicaciones. No toda la información se encuentra disponible para los usuarios que lo necesitan. Esto fue validado con los operadores del centro de cómputo personal encargado de monitorear y operar aplicaciones, servicios ejecución de procesos y respaldos

Recomendaciones

Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

5.1.1.1.4.2.16 Monitoreo y revisión de los servicios de Terceros (A.10.2.2)

Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

Hallazgos

El cumplimiento de este control es parcial ya que solo se lleva acabo el monitoreo en los enlaces de datos en los proveedores. Se verifico este cumplimiento con los registros de bitácoras indicadas del jefe del área de redes

Recomendaciones

Se sugiere tener un mayor control en los servicios que se obtiene de terceros y llevar un registro y ser evaluado los servicios que proporcionan periódicamente.

5.1.1.1.4.2.17 Controles contra software malicioso (A.10.4)

Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.

Hallazgos

Se posee software y equipos apropiado para la detección, prevención y recuperación que protege en un alto nivel de los códigos maliciosos.

Falta la capacitación a los usuarios sobre la seguridad de la información. Que fue verificado según los planes de capacitación que tiene el personal

Recomendaciones

Emitir charlas periódicas al personal sobre la seguridad de la información.

5.1.1.1.4.2.18 Controles contra códigos móviles (A.10.4.2.2)

Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado

Hallazgos

En la actualidad MDMQ no cuenta con políticas de seguridad para código móvil esto fue indicado por el jefe de desarrollo de aplicaciones.

Recomendaciones

Creación de políticas de seguridad que controle este tipo de código

5.1.1.1.4.2.19 Back-up o respaldo de la información (A.10.5.1)

Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.

Hallazgos

Los backups se realizan ciertas bases de datos, máquinas virtuales, aplicativas, servicios, configuración servidores, equipos del Data Center y elementos de telecomunicaciones y redes.

No existe un documento donde se establezca las políticas de respaldo de los elementos.

Los respaldos que se generan, no son probados regularmente con un procedimiento formal esto fue validado con el personal del centro de cómputo como con los administradores de la infraestructura tecnológica.

Recomendaciones

Priorizar los respaldos esenciales que son indispensables tanto de los aplicativos, servicios y configuraciones. Una vez realizada esta priorización se debe generar un documento donde se establezca las políticas de respaldos que se va a realizar sobre cada uno de estos elementos involucrados.

Los respaldos generados deben ser validados para comprobar su integridad al menos cada mes.

5.1.1.1.4.2.20 Seguridad de los servicios de red (A.10.6.2)

Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.

Hallazgos

Se cumple parcialmente porque el equipamiento tiene contratos de garantía técnica donde existen niveles de servicio.

Recomendaciones

En los contratos y garantías con servicios externos se deben reducir a tiempos de soportes mínimos para evitar la pérdida de servicio

5.1.1.1.4.2.21 Eliminación de medios (A.10.7.2)

Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.

Hallazgos

Los equipos del data center, servidores, equipos de red son reemplazados cuando cumple su vida útil de funcionamiento, pero la información que contenía no se da una adecuada eliminación de su información que posee. Esto fue validado por los responsables de la infraestructura tecnológica.

Recomendaciones

Antes de ser eliminado cualquier medio se debe realizar procedimientos para el borrado total de la información que pose, para evitar la lectura de datos que posee.

5.1.1.1.4.2.22 Procedimientos de manejo de la información (A.10.7.3)

Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.

Hallazgos

El control se cumple en gran parte porque en los servidores de archivos se maneja en esquemas de permisos y en los respaldos el acceso en restringido. Los permisos son asignados según requerimientos enviados al sistema de mesa de ayuda.

Recomendaciones

Se recomienda levantar el servicio de auditoria sobre los acceso a los respaldos y a los servidores de archivos con el fin de tener detallado su manejo.

5.1.1.1.4.2.23 Procedimientos y políticas de información y Software (A.10.8.1)

Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.

Hallazgos

El control se cumple parcialmente porque existen varios intercambios de información informalmente esto fue validado según los procesos que manejan en el centro de cómputo con el personal de operación.

Recomendaciones

Se recomienda poseer un procedimiento formal para el intercambio de información donde quede de alguna forma constancia del uso de la misma.

5.1.1.1.4.2.24 Mensajes electrónicos (A.10.8.4)

Se debe proteger adecuadamente los mensajes electrónicos.

Hallazgos

El servicio de correo electrónico institucional es manejado con copias de sus mensajes electrónicos en sus equipos locales se validó con varios usuarios de diferentes áreas que manejan archivos locales de sus correos en sus computadores.

Recomendaciones

No poseer copias en los equipos locales. Todos los mensajes electrónicos de los usuarios deben estar alojados en un espacio común, protegidos y resguardados con apropiadas seguridades.

5.1.1.1.4.2.25 Información disponible públicamente (A.10.9.3)

Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.

Hallazgos

La información pública se tiene mínimamente protegida, esto fue comprobado en las carpetas compartidas con información pública que tiene permisos de escritura.

Recomendaciones

Proteger este tipo de información para mantener la integridad de la información pública expuesta a la ciudadanía

5.1.1.1.4.2.26 Registro de auditoria (A.10.10.1)

Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

Hallazgos

Se comprobó con los administradores que se tiene activado los registros de auditoria en ciertas aplicaciones, equipos del data center, servicios, equipos de redes pero a menudo estas actividades se sobre escriben con las actividades nuevas registradas con lo cual no se puede realizar investigaciones de eventos pasados.

Recomendaciones

Activar los registros de auditoria de los servicios, aplicativos, servidores, equipos de red. Además de establecer un periodo de retención de esos registros almacenados para poder realizar un análisis de los eventos.

5.1.1.1.4.2.27 Registros del administrador y operador (A.10.10.4)

Se deben registrar las actividades del administrador y operador del sistema.

Hallazgos

Existen bitácoras donde los administradores y operadores de los sistemas registran sus actividades. Pero el uso de cuentas genéricas por estas personas afecta la identificación sus actividades y la verificación de las acciones realizadas.

Recomendaciones

Poseer cuentas por cada responsable de los administradores como operadores de los sistemas, además la activación de las auditorias de los sistemas y programas para el registro de las actividades realizadas sobre estos.

5.1.1.1.4.2.28 Registro de falla (A.10.10.5)

Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.

Hallazgos

Las fallas de los sistemas solo son analizadas el momento de producirse algún inconveniente hasta encontrar el motivo de este esto es validado por los administradores de los sistemas, infraestructura, aplicaciones, equipos red y equipamiento del center. Pero no se documentados para poseer un registro de estas actividades.

Recomendaciones

Se debe registrar en todo momento las actividades de errores y fallas con esto generar una base de conocimiento. Para poder identificar me mejor manera las acciones sobre esos problemas presentados.

5.1.1.1.4.2.29 Sincronización de Relojes (A.10.10.6)

Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.

Hallazgos

Los servidores Windows y computadoras de escritorios se sincronizan automáticamente con un servidor NTP interno.

Los servidores Linux, equipos del Data, de telecomunicaciones y otros elementos no están configurados la sincronización de los relojes o lo toman de otras fuentes externas

Recomendaciones

Se debe establecer que el único elemento de sincronización de relojes en el servidor de tiempo interno.

5.1.1.1.4.2.30 Inscripción del usuario (A.11.2.1)

Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.

Hallazgo

El control cumple en gran parte porque todos los procedimientos se encuentran establecidos en las políticas la asignación de accesos a los sistemas se lo realiza en varias áreas.

Este procedimiento de asignación de accesos es asignado mediante un requerimiento de la mesa de ayuda a los diferentes responsables.

Recomendación

Se recomienda generar un manual de procedimiento para otorgar acceso a todos los sistemas que otorga la DMI.

5.1.1.1.4.2.31Gestión de privilegios (A.11.2.2)

Se debe restringir y controlar la asignación y uso de los privilegios.

Hallazgo

El control se cumple parcialmente porque a nivel jerárquico que es imposible controlar los privilegios, a nivel operativo si existe control de asignación de privilegios.

Recomendación

Se recomienda generar una política donde no importe el tipo de jerarquía que posee tenga las obligaciones se deben cumplir a todo nivel.

5.1.1.1.4.2.32 Revisión de los derechos de acceso del usuario (A.11.2.4)

La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

Hallazgo

El control se cumple de forma parcial ya que para acceder a los sistemas se solicita un oficio, pero esto no es evaluado de forma regular esto es evidenciado con personal de mesa de ayuda quien asigna los requerimientos.

Recomendación

Se recomienda concebir una política para la revisión de los permisos de accesos sobre todos en los sistemas más críticos o accesos físicos.

5.1.1.1.4.2.33 Uso de clave (A.11.3.1)

Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.

Hallazgo

Se observó que este control se cumple de forma parcial ya que los usuarios no poseen buenas prácticas de seguridad. Existen usuarios poseen claves muy básicas de seguridad.

Recomendación

Se recomienda crear políticas de buenas prácticas de para la creación de claves robustas, además de dar charlas y talleres sobre temas de seguridad.

5.1.1.1.4.2.34 Política de pantalla y escritorio limpio (A.11.3.3)

Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.

Hallazgo

Se cumple parcialmente no se tiene una política para que el personal al terminar sus labores deje documentos con información sensible de trabajo lo almacenen en un lugar seguro.

Recomendación

Crear un manual de buenas prácticas donde consten política que los documentos sensibles deben siempre ser almacenados en lugares seguros.

5.1.1.1.4.2.35 Identificación y autenticación del usuario (A.11.5.2)

Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.

Hallazgo

A nivel de usuarios todos tienen un identificador único, los Administradores del departamento de infraestructura manejan perfiles administradores. Toda autenticación se la realiza por Active Directory.

Recomendación

Los Administradores de Infraestructura deberían utilizar sus perfiles para tener su identificador de las acciones que realiza.

5.1.1.1.4.2.36 Sistema de gestión de claves (A.11.5.3)

Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.

Hallazgo

No existe un manejo de claves interactivas, estas se las crea a criterio personal de los responsables de los sistemas, aplicaciones, equipos, etc. De igual manera la calidad de las claves queda en el criterio personal

Recomendación

Se debe generar una política para el manejo de claves. Estableciendo criterios con niveles de seguridad para la creación de estas.

5.1.1.1.4.2.37 Uso de utilidades del sistema (A.11.5.4)

Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.

Hallazgo

La mayoría de usuarios manejan perfiles con accesos restringidos con lo cual no pueden realizar cambios, pero los Administradores de los aplicativos, servicios y servidores utilizan perfiles superiores, con este perfil se puede realizar cualquier tipo de cambios.

Recomendación

Todos los usuarios deben utilizar perfiles básicos para evitar el mal uso de los programas.

5.1.1.1.4.2.38 Uso de utilidades del sistema (A.11.7.1)

Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.

Hallazgo

Para dispositivos como celulares y tablas no existe ninguna política para protegerlos contra riesgos de seguridad

Recomendación

Adoptar política de seguridad para todos los nuevos dispositivos móviles que existen en la actualidad y estos consten en el documento de políticas de gestión de información.

5.1.1.1.4.2.39 Tele-trabajo (A.11.7.2)

Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.

Hallazgo

Existe personal que trabaja desde su casa, pero no existe una política regulatoria sobre dicho tema.

Recomendación

Crear políticas y regulaciones sobre este tipo de trabajo que se puede realizar desde otros lugares ajenos a la Institución.

5.1.1.1.4.2.40 Control de software operacional (A.12.4.1)

Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.

Hallazgo

Está controlado en gran medida en servidores de producción pero en equipos de desarrollo pueden instalar cualquier tipo de software.

Recomendación

Se debe instalar solamente software que se tenga licenciado y se debe realizar el checklist de pruebas de los sistemas.

5.1.1.1.4.2.41 Procedimientos de control de cambio (A.12.5.1)

La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.

Hallazgo

Existe control de cambios a lo referente a aplicativos, pero no se lleva un control de cambios que se refiere a los servicios de terceros, equipamiento del data center, equipos de redes, servidores.

Recomendación

Cada responsable debe entregar al departamento de delivery el Control de Cambios de aplicativos, que es un documento donde se registra los cambios o actualizaciones que se realiza tanto en los elementos de red, servidores, equipamiento del data center con esto se tendrá un mejor control sobre la infraestructura del data center.

5.1.1.1.4.2.42 Revisión técnica de las aplicaciones después de cambios en el sistema operativo (A.12.5.2)

Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.

Hallazgo

El control cumple parcialmente porque se tiene un esquema de verificación pero a veces no se cumple por parte de los usuarios.

Recomendación

Se observa de una forma preocupante que no se toma en cuenta la criticidad de no cumplir con las pruebas respectivas antes de poner en producción los sistemas y los problemas adversos que se puede ocasionar al no realizar un Informes Técnicos donde se detalla las actividades a realizar y su afectación.

5.1.1.1.4.2.43 Control de vulnerabilidades técnicas (A.12.6.1)

Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

Hallazgo

Este control no se cumple porque se encuentran las personas operando con el día a día

Recomendación

Se observa que no hacen pruebas de infiltración las cuales es muy preocupante ya que las personas no son proactivas sino reactivas y no realizan estas actividades que son vitales para una organización.

5.1.1.1.4.2.44 Responsabilidades y procedimientos (A.13.2.1)

Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

Hallazgo

El control se aplica parcialmente porque no existe una política generada para este tipo de casos por lo que solo se aplica empíricamente.

Recomendación

Se recomienda crear una política y ser registrada en el documento de Políticas de gestión de información, para el manejo de procedimientos gerenciales y comunicar el manejo.

5.1.1.1.4.2.45 Aprendizaje de los incidentes en la seguridad de la información (A.13.2.2)

Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.

Hallazgo

No se tiene una evolución de que permita cuantificar y monitorear los volúmenes y costos de los incidentes de la seguridad de la información.

Recomendación

Se recomienda crear un mecanismo en el cual se pueda evidenciar la evolución cuantitativa del impacto de los incidentes de seguridad en los parámetros ya mencionados.

5.1.1.1.4.2.46 Incluir seguridad de la información en el proceso de gestión de continuidad comercial (A.14.2.1.1)

Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.

Hallazgo

Se debe crear una política donde se defina una el plan de continuidad de negocio ya que no se posee un plan definido y aprobado por las autoridades y se realizan tareas empíricamente.

Recomendación

Se recomienda realiza un plan de continuidad de negocio de forma que toda la información sea salvaguardada.

5.1.1.1.4.2.47 Continuidad comercial y evaluación del riesgo (A.14.2.1.2)

Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

Hallazgo

El control se cumple parcialmente ya que se identifica pero no se realiza un análisis de impacto, probabilidad y el análisis de las consecuencias.

Recomendación

Se recomienda de forma vital el análisis y el impacto de cada uno de los riesgos y tomar decisiones sobre ellos y dar el respectivo seguimiento del mismo.

5.1.1.1.4.2.48 Marco referencial para la planeación de la continuidad comercial (A.14.2.1.4)

Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.

Hallazgo

Se posee un contrato de mantenimiento de la plataforma del Data Center. No se tiene solo un marco de referencias ya que no se posee un BCP.

Recomendación

Se recomienda que se cree y se determine un periodo de actualización y revisión del BCP.

5.1.1.1.4.2.49 Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales (A.14.2.1.5)

Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.

Hallazgo

El control se cumple parcialmente porque no se actualiza continuamente.

Recomendación

Se recomienda que se cree una política en la cual se determine un periodo de actualización y revisión del BCP.

5.1.1.1.4.2.50 Identificación de legislación aplicable (A.15.1.1)

Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.

Hallazgo

El control se cumple parcialmente porque este tipo de documentación lo realiza a veces el área interesada.

Recomendación

Se recomienda generar una política de documentación y estas estén registradas en las políticas de gestión de información, ya que son formas de direccionar y pueden ser un referente para las siguientes intervenciones.

5.1.1.1.4.2.51 Derechos de propiedad intelectual (IPR) (A.15.1.2)

Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.

Hallazgo

El control se cumple parcialmente porque no existe una evaluación periódica de levantamiento de información donde consten un listado de programas licenciados o programas desarrollados y que solo estos estén instalados en los diferentes equipos.

Recomendación

Se recomienda generar una política de revisión de los contratos donde se evalué el cumplimiento del mismo y esté puede ser aleatoriamente, y verificar que en los equipos solo sea utilizado programas licenciados o permitidos.

5.1.1.1.4.2.52 Protección los registros organizacionales (A.15.1.3)

Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

Hallazgo

El control se cumple parcialmente porque no existe una política de protección de registros de la organización, contra pérdida, destrucción y falsificación.

Recomendación

Se recomienda generar una política que respalde este tipo de información y que no se sabe cuándo se la pueda utilizar.

5.1.1.1.4.2.53 Protección de data y privacidad de información personal (A.15.1.4) Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

Hallazgo

El control se cumple parcialmente porque cada funcionario tiene equipos con sus respectivas claves del Directorio Activo.

Recomendación

Se recomienda generar políticas de seguridad que sean descritas en las políticas de gestión de Información y realizar talleres de sociabilización a las personas sobre seguridad y las consecuencias.

5.1.1.1.4.2.54 Prevención de mal uso de medios de procesamiento de información (A.15.1.5).

Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.

Hallazgo

El control cumple parcialmente porque aunque no se tiene establecido en un reglamento formal el utilizar herramientas municipales para fines propios se lo realiza empíricamente.

Recomendación

Se requiere generar un reglamento d manejo de bienes informáticos donde se detalle todo este tipo de actividad.

5.1.1.1.4.2.55 Cumplimiento con las políticas y estándares de seguridad (A.15.2.1)

Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.

Hallazgo

El control se cumple parcialmente ya que las políticas y normativas existen para algunos casos no se cumplen por aspectos de urgencia.

Recomendación

Se recomienda generar una política de cumplimiento que se encuentre descrita en las Políticas de gestión de Información o en el manual de procedimientos de seguridad, sobre las modificaciones o procesos los cuales deben ser planificados con tiempo para no realizar los procesos inadecuados como saltarse los pasos de prueba.

5.1.1.1.4.2.56 Chequeo de cumplimiento técnico (A.15.2.2)

Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.

Hallazgo

No se posee una Política clara de monitoreo de los sistemas de información porque solo se los monitorea cuando existe un reporte de lentitud o las funcionamiento.

Recomendación

La forma correcta de llevar acabo un monitoreo es cuando se lo realiza planificada mente y bajo un periodo determinado y los resultados son registrados en una bitácora de novedades.

5.1.1.1.4.2.57 Controles de auditoria de sistemas de información (A.15.3.1)

Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.

Hallazgo

No se posee los requerimientos de auditoria sobre los sistemas operativos de los servidores, equipos de red.

Recomendación

Crear un cronograma un plan de auditoria para el chequeo de los sistemas operativos de los servidores y equipos de red

5.1.1.1.4.2.58 Protección de las herramientas de auditoria de los sistemas de información (A.15.3.2)

Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Hallazgo

Existen herramientas de monitoreo de los sistemas pero solo de ciertos aplicativos no hay de todos y no se tiene una idea clara de su buen o mal funcionamiento, solo su actividad a nivel general lo cual en caso de un problema no se tiene como determinar en forma precisa.

Recomendación

Definir de una forma correcta el monitorear por aplicativo ya que si no se tiene una idea clara de cómo está el funcionamiento individual puede que se tenga alguna falla y no se podrían solucionarlo de forma correcta y efectiva.

5.1.2.1.4.3 Hallazgos encontrados en el análisis de auditoria que no constan en la matriz de la ISO 27001:2005

5.1.2.1.4.3.1 Problema sobre obtención de respaldos

No se realiza Backups de elementos de configuración de aplicaciones

Hallazgos

No se cuenta con respaldo de configuraciones de las aplicaciones críticas con la que cuenta el MDMQ, lo referente a la data si se tiene respaldos diarios.

Sistema de Pagos de Impuestos a través de la Banca y Cooperativas, Sistema Integrado de Registro catastral de Quito – SIRECQ, Sistema de pagos de impuestos a través de tarjetas de crédito, Sistema de seguridad y personas, Sistema SAO, LUAE – BPM, Sistema de administración de requerimientos - GDOC, Sistema territorial IRM informe regulación metropolitana, Sistema territorial SGCT Sistema de gestión de la construcción Territorial, SAO-Patentes, Rehosting, SISTEMA SIABIM, Sistema SIABIP

Recomendaciones

Obtener los respaldos de las aplicaciones más críticas con sus archivos de configuraciones al menos dos veces a la semana o cuando se realice algún cambio drástico de configuración de estos elementos. Con el fin de realizar una recuperación inmediata del aplicativo.

5.1.2.1.4.3.2 Mantenimientos preventivos

Realizar mantenimientos periódicos

Hallazgos

No se realizan mantenimientos periódicos de los elementos críticos del data center como son: la librería de respaldos, aire acondicionado, generador eléctrico, panel de incendios

Recomendaciones

Realizar mantenimientos periódicos al menos cada tres meses de los elementos críticos del data center para evitar su degradación o fallos.

5.1.2.1.4.3.3 Equipos de telecomunicaciones

No contar con contingencia en ciertos equipos de telecomunicaciones

Hallazgos

Se identificado que los equipos de telecomunicaciones: Wimax controlador, Wimax radio bases, ons no poseen contingencias, al momento de subir avería el servicio se vería afectado sin un tiempo aceptable de recuperación.

Recomendación

Contar con esquemas de alta disponibilidad para estos equipos de telecomunicaciones.

5.1.2.1.4.3.4 Aplicación de actualizaciones

Respaldos de configuraciones y actualizaciones a los servidores

Hallazgos

Se ha identificado que en algunos casos los servidores del data center: encluseribm chasis e, encluser hp c3000, storage ds-3400,storage p6500(1),storage p6500(2),storage p2000(1), encluseribm chasis h, encluser hp c700 no poseen las últimas actualizaciones.

Además no se cuenta con respaldos de las configuraciones de estos equipos.

Recomendaciones

Establecer un esquema de actualizaciones sobre los servidores y mantener las últimas actualizaciones estables sobre estos equipos.

Establecer un plan de respaldos para obtener las configuraciones de estos equipos al menos una vez por semana o cuando se realiza un cambio crítico sobre las configuraciones.

5.1.1.1.5 Conclusiones

La falta de la implementación oportuna de un sistema de gestión de la seguridad de la información (SGSI) como un estándar establecido de cumplimiento obligatorio que contenga normas, estándares para analizar, describir, valorar clasificar acciones y responsabilidades dificulta el cumplimiento a políticas de seguridad y procedimiento adecuado que sumen valor agregado o contribuya al buen desarrollo y superación de la Dirección de Informática.

Al no realizar auditorías a los procesos de seguridad no se posee una idea clara de cómo se encuentran y el estado de cumplimiento si se ha mejorado o empeorado el cumplimiento de los controles.

La falta de un Data Center alterno puede ser la causa de que si se da un evento fortuito con el Data Center, se tenga tiempos muy altos o en el peor de los casos catastróficos la restauración de los servicios para la atención al público.

En Dirección Metropolitana de Informática no cuenta con área especializada de seguridad de la información, que dicte las normas y políticas para el manejo adecuado de la información.

En el Municipio del Distrito Metropolitano de Quito a pesar que se cuenta con documentación sobre sobre políticas de seguridad de la información aprobadas

por los más altos mandos de la organización, este documento no registra actualizaciones sobre los nuevos modelos de seguridad de la información que existen en la actualidad.

Se debe clasificar los tipos de información que se posee (critica, confidencial, sensible, publica) que se encuentra en el MDMQ.

Se resguarda los datos de los sistemas, pero no se posee un adecuado plan de respaldos sobre aplicaciones ni configuraciones de equipos. Además de no contar con un proceso para la validación de respaldos.

5.1.1.1.6 Recomendaciones

Mediante un comité de seguridad que maneje de buena manera el desarrollo y cumplimiento de las políticas de la Dirección de Informática debe realizar un proyecto de implantación del SGSI de un sistema de gestión de la seguridad de la información (SGSI), para garantizar que solo se efectúen operaciones y procedimiento establecidos.

Se debe mantener una política de mejoramiento continuo mediante auditorías a los procesos de seguridad que son de gran impacto e importancia para el Data Center y la Dirección de Informática ya que la criticidad y el buen manejo de la información deben tener prioridad.

Se debe revisar los convenios interinstitucionales los cuales permitan tener un Data Center alterno, lo cual si se suscita un evento catastrófico se pueda tener una restauración completa y oportuna de los servicios al público.

Se debe establecer procesos de seguridad de la información por grupos especializados de profesionales que den el cumplimiento de las mejoras prácticas de seguridad.

Se debe establecer un proceso de mejoramiento continuo sobre el documento de políticas de gestión tecnológicas a cargo de un comité especializado.

Los dueños de la información son los encargados de establecer y etiquetar los tipos de información que poseen. Y dependiendo el tipo de información establecer procesos para resguardarla.

Se debe ejecutar procesos de respaldos de configuraciones tanto de aplicativos y equipos críticos. Además de contar con un sitio alterno para resguardar todo los respaldos obtenidos. Establecer una validación periódicamente de los últimos respaldos obtenidos.

Capítulo VI

6.1 Conclusiones y Recomendaciones

6.1.1 Conclusiones

Una vez concluida el trabajo de investigación se pudo conocer de forma clara el cumplimiento de los controles de seguridad que posee el Data Center de la Dirección Metropolitana de Informática con relación a las normas ISO 27001:2005 e ISO 27002:2005.

El personal del Municipio Metropolitano de Quito a pesar que cuenta con políticas de gestión tecnológicas no tiene una conciencia sobre la seguridad de la información. Por tal motivo se puede producirse fugas de información crítica confidencial.

En base a lo investigado se ha identificado que los procesos de seguridad establecidos actualmente en el Data Center no poseen una evaluación continua.

Con esta investigación se concluye que la información sensible y critican o se encuentra alojada únicamente en el Data Center de la Dirección Metropolitana de Informática sino se encuentra también dispersa en otras dependencias.

6.1.2 Recomendaciones

Contar con un cronograma de concientización sobre la seguridad de la información a todo el personal del Municipio del Distrito Metropolitano de Quito.

Se debe formalizar en el documento de políticas institucionales todos los procedimientos de seguridad de la información.

Realizar un cronograma para la evacuación de los procesos de seguridad de la información y los hallazgos encontrados deben ser conocidos por los directivos para posterior implantación y luego deberán ser nuevamente evaluados verificar su efectividad.

Se recomienda identificar las áreas que interviene en el manejo de información crítica y sensible en cada una de las dependencias del Municipio de Quito, creando procedimientos para asegurarlas.

La adopción de la seguridad de la información es un tema muy importante que en la actualidad grandes empresas a nivel nacional e internacional están implementando para proteger su información.

Bibliografía

aglone3. (Julio de 2012). *Responsabilidad sobre los activos*. Obtenido de Responsabilidad sobre los activos: https://iso27002.wiki.zoho.com/7-1-Responsabilidad-sobre-los-activos.html.

aglone3. (Julio de 2012). *Seguridad Física y del Entorno*. Obtenido de Seguridad Física y del Entorno: https://iso27002.wiki.zoho.com/9-1-%C3%81reas-seguras.html.

aglone3. (Julio de 2013). *Adquisición, Desarrollo y Mantenimiento de Sistemas de Información*. Obtenido de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información: https://iso27002.wiki.zoho.com/12-1-Requisitos-de-seguridad-de-los-sistemas.html

aglone3. (Julio de 2013). *Identificación de la legislación aplicable*. Obtenido de Identificación de la legislación aplicable: https://iso27002.wiki.zoho.com/15-1-1-Identificaci%C3%B3n-de-la-legislaci%C3%B3n-aplicable.html

aglone3. (Julio de 2013). *Organización Interna*. Obtenido de Organización Interna: https://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html.

aglone3. (Julio de 2013). *Política de seguridad de la información*. Obtenido de Política de seguridad de la información: https://iso27002.wiki.zoho.com/5-1-Pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html.

aglone3. (Julio de 2013). *Procedimientos y responsabilidades de operación*. Obtenido de Procedimientos y responsabilidades de operación: https://iso27002.wiki.zoho.com/10-1-Procedimientos-y-responsabilidades-de-operaciC3%B3n.html.

aglone3. (Julio de 2013). *Proceso de la gestión de continuidad del negocio*. Obtenido de Proceso de la gestión de continuidad del negocio: https://iso27002.wiki.zoho.com/14-1-1-Proceso-de-la-gesti%C3%B3n-de-continuidad-del-negocio.html.

aglone3. (Julio de 2013). *Requerimientos de negocio para el control de accesos*. Obtenido de Requerimientos de negocio para el control de accesos: https://iso27002.wiki.zoho.com/11-1-Requerimientos-de-negocio-para-el-control-de-accesos.html

aglone3. (Julio de 2013). *Seguridad en la definición del trabajo y los recursos*. Obtenido de Seguridad en la definición del trabajo y los recursos: https://iso27002.wiki.zoho.com/8-1-Seguridad-en-la-definici%C3%B3n-del-trabajo-y-los-recursos.html.

AS/NZS 4360(1999). (1999). *Estándar australiano administración de riesgos.*

Departamento de Comunicación. (Agosto de 2013). *ValdezAlbizu informa Banco Central obtiene certificación ISO 27001*. Obtenido de ValdezAlbizu informa Banco Central obtiene certificación ISO 27001: http://www.bancentral.gov.do/notas_del_bc.asp?a=bc2012-05-30.

Estándar internacional ISO/IEC. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información- Requerimientos.*

Estándar internacional ISO/IEC17799 - 27002. (2005). *ecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.*

Estándar internacional ISO/IEC27001. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información - Requerimientos.*

ISO 31000. (2009). *Gestión de riesgo– principios y guías.*

Quezada. (2012). *Base de datos. Recuperado*. Obtenido de Base de datos. Recuperado: http://es.scribd.com/doc/119813298/Telconet.

Quito, M. d. (2011). *Plan de desarrollo 2012 - 2022.* Quito.

Anexos