PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TRABAJO DE GRADO

"ANÁLISIS DE RIESGO TECNOLÓGICO DEL CENTRO DE DATOS BASADO EN NORMAS INTERNACIONALES: CASO GADMCE"

LÍNEA DE INVESTIGACIÓN:
GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

PREVIA OBTENCIÓN DEL TÍTULO:
INGENIERA DE SISTEMAS Y COMPUTACIÓN

AUTORA: GUADALUPE ROCÍO CHIPANTIZA SIFUENTE

ASESOR: ING. KLEBER VERA

Esmeraldas, Ecuador, Enero de 2018

Disertación aprobada luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de grados de la PUCESE, previo a la obtención del título de Ingeniera en Sistemas y Computación.

TRIBUNAL DE GRADUACIÓN

Título:

"Análisis de riesgo tecnológico del centro de datos basado en normas internacionales: Caso GADMCE**"**

Autor: Guadalupe Rocío Chipantiza Sifuente

Ing. Kleber Vera **f.-……**

Asesor

Mgt. Susana Patiño : **f.- ……..**

Lector

Mgt.Cesar Godoy : **f.- ……..**

Lector

Mgt. Xavier Quiñonez Ku: **f.- ……..**

Director de Escuela

Ing. Maritza Demera Mejía **f.- ……....**

Secretaria General PUCESE

Esmeraldas, Ecuador, Enero 2018

CERTIFICADO DE TUTORÍA

Ing. Kleber Vera, docente investigador de la PUCESE.

CERTIFICO:

Que el trabajo de grado titulado **"**ANÁLISIS DE RIESGO TECNOLÓGICO DEL CENTRO DE DATOS BASADO EN NORMAS INTERNACIONALES: CASO GADMCE**",** realizado por GUADALUPE ROCÍO CHIPANTIZA SIFUENTE ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la PUCESE, en el reglamento de Estudiantiles de la Pontificia Universidad Católica del Ecuador Sede en Esmeraldas.

Debido a que reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final, las sugerencias realizadas, en consecuencia, está en condiciones de ser sometido a la valoración del Tribunal encargado de juzgarla.

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

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, a Enero de 2018

Ing. Kleber Vera
ASESOR

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Guadalupe Rocío Chipantiza Sifuente, portadora de la cédula de identidad No. 0802113332, declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de **Ingeniera en Sistemas y Computación** son absolutamente originales, auténticos y personales.

En tal virtud, declaro que ha sido desarrollado con base a una investigación exhaustiva, contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

Guadalupe Rocío Chipantiza Sifuente
CI. 0802113332

AGRADECIMIENTO

Protagonista principal y por quien me siento muy agradecida Dios que me ha brindado momentos felices y a la vez momentos que ha fortalecido mi vida, enseñanza adquirida en el trayecto del tiempo, brindándome salud, vida y la capacidad para adquirir nuevos conocimientos naturales y científicos que fortalecieron mi formación académica.

Agradezco a mis padres María Elena Sifuente y Segundo Chipantiza por su cariño, enseñanzas y sabiduría que me fomentaron en mi desarrollo como persona, siendo una herramienta de mi vida desde la niñez.

Agradezco a José Eduardo Luna por su apoyo y comprensión los cuales ha sido muy importante para seguir luchando en esta meta propuesta.

Agradezco al Ing. Kleber Vera, Asesor de Tesis; Ing. Susana Patiño, Ing. Cesar Godoy, Lectores de Tesis; demás maestros y compañeros de aulas quienes depositaron en mí sus sabias enseñanzas y apoyo incondicional para llegar al feliz término de este proyecto.

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

A todos ellos muchas gracias.

Guadalupe Chipantiza Sifuente

DEDICATORIA

Este presente trabajo va dirigido en primer lugar a Dios, por ser mi iluminación y fe en perseverar para poder cumplir con la tesis

A mis hijos Josué, Nayeli y Adrián a quienes adoro muchísimo, son mi fortaleza y son quienes dan luz a cada proyecto propuesto.

A José Eduardo Luna quien me dio el empuje constantemente para poder desarrollar mi tesis, quien no dudo en regañarme para obtener la culminación de mi tesis, a quien digo ESTA LISTA LA TESIS

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

Esto y mucho más para ustedes, cariñosamente,

Guadalupe Chipantiza Sifuente

ÍNDICE GENERAL

Contenido

CERTIFICADO DE TUTORÍA iii
DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD iv
AGRADECIMIENTO v
DEDICATORIA vi
RESUMEN xi
ABSTRACT xii
INTRODUCCIÓN 1
1.1 Presentación de la investigación 1
1.2 Planteamiento del problema 1
1.3 Justificación del estudio 2
1.4 Objetivos 4
CAPITULO I: MARCO DE REFERENCIA 5
1.4.1. Antecedentes (Estudios previos) 5
1.4.2. Bases teóricas científicas 6
1.4.3. Marco Legal 19
CAPITULO II: MATERIALES Y MÉTODOS 21
2.1. Descripción del lugar 21
2.1.1. Ubicación 21
2.2. Métodos y técnicas 21
2.3. Población 22
2.4. Técnicas de procesamiento y análisis de datos 22
2.5. Normas éticas 23
CAPÍTULO III: RESULTADOS 24
3.1. Análisis e interpretación de resultados 24
CAPÍTULO IV: PROPUESTA DE INTERVENCIÓN 26
4.1. Análisis de Riesgo Tecnológico del Centro de Datos del GADMCE basado en normas internacionales. 26
4.1.1. Calificación de la probabilidad e impacto del centro de datos del GADMCE 29
4.1.2. Intervalos de riesgos de los activos del centro de datos del GADMCE 33
4.1.3. Priorización de los activos del centro de datos del GADMCE según riesgos 33
4.1.4. Evaluación aplicando controles según Norma ISO/IEC 27002 35
4.1.5. Informe de Auditoria 37

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 42
5.1. Conclusiones 42
5.2. Recomendaciones 42
REFERENCIAS 44
6.1. Referencias bibliográficas 44
6.2. Anexos 47

ÍNDICE DE TABLAS

Tabla 1. Dispositivos de Infraestructura de TI 10
Tabla 2. Elementos básicos de un data center 12
Tabla 3. Aplicación de la Norma ICREA 2013 30
Tabla 4. Escala de probabilidad de falla de activo 30
Tabla 5. Escala de impacto en activos 31
Tabla 6. Matriz de riesgo del centro de datos del GADMCE 34
Tabla 7. Intervalos de riesgos para activos del centro de datos 34
Tabla 8. Priorización de riesgos del centro de datos GADMCE 35
Tabla 9. Prioridad de riesgo 36
Tabla 10. Cuadro de controles para riesgos 37

ÍNDICE DE FIGURAS

Figura 1. Orgánico Estructural GADMCE …….. 7
Figura 2. Estructura de Unidad de Sistema…….. 8
Figura 3. Topología de Red National Experts S.A. …… 15
Figura 4. Análisis y gestión de Riesgos en una organización ……... 21
Figura 5. Ubicación geográfica del GADMCE …….. 23
Figura 6. Servidores…… …….. 52
Figura 7. Tablero principal…….. 53
Figura 8. Tablero de transferencia…….. 54
Figura 9. Aire acondicionado básico…….. 55
Figura 10. Servidores toma de lejos …….. 56
Figura 11. Racks y UPS…….. 57
Figura 12. UPS…….. 58
Figura 13. Equipo Cisco …….. 59
Figura 14. Equipo Cisco y Cloud Mikrotik …….. 60
Figura 15. Etiquetas en el cableado …….. 61
Figura 16. Captura de pantalla del sistema de monitoreo…….. 62
Figura 17. Diagrama Unifilar de red eléctrica…….. 63

RESUMEN

El presente trabajo de investigación parte del estudio del sistema, herramientas informáticas y técnicas de seguridad de la información digital organizacional del Centro de Datos del Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas (GADMCE), con la finalidad de detectar las debilidades y necesidades existentes; y en base a ello, formular una propuesta de mejora. La importancia del estudio reside en las crecientes amenazas (tanto internas como externas) existentes en el sector informático, un sector en expansión y que demanda por parte de los organismos oficiales el diseño y mantenimiento de controles de seguridad de la información digital. La detección temprana de amenazas o posibles riesgos minimiza los mismos; mientras que la pérdida de información almacenada podría ocasionar graves consecuencias en el funcionamiento siendo que el GADMCE tiene a custodia información sensible de la ciudadanía, entre ellos información catastral, permisos de funcionamiento para las actividades económicas, pagos de impuestos prediales, patentes entre otras, información delicada la cual se encuentra alojada en los servidores y sistemas de almacenamiento ubicado en el centro de datos; por lo que se debe implementar protocolos de seguridad basados en normas internaciones en las administraciones públicas. La información concerniente a la detección de las debilidades y riesgos existente en el Centro de Datos del GADMCE se orienta bajo la evaluación técnica para especificar el cumplimiento según las normas ISO/IEC 27002 e ICREA 2013 y se tendrá mediante la realización de entrevistas a profundidad al personal de mantenimiento técnico de Sistemas del GADMCE, que tienen relación directa con esta infraestructura, con el propósito de conocer cómo se administra el centro de datos, observando el mejoramiento continuo de la seguridad.

PALABRAS CLAVES: CENTRO DE DATOS, GADMCE, RIESGO TECNOLÓGICO, ESTÁNDARES.

ABSTRACT

The present research work is based on the study of the system, computer tools and security techniques of the digital organizational information of the Data Center of the Autonomous Decentralized Municipal Government of the Esmeraldas Canton (ADMGEC), with the purpose of detecting the existing weaknesses and needs; and based on this, formulate a proposal for improvement. The importance of the study lies in the growing threats (both internal and external) in the IT sector, an expanding sector that demands the design and maintenance of digital information security controls by official organizations. The early detection of threats or possible risks minimizes them; while the loss of stored information could cause serious consequences in the operation being that the ADMGEC has to custody sensitive information of the citizenship, including cadastral information, operating permits for economic activities, property tax payments, patents among others, information delicate which is hosted in the servers and storage systems located in the data center; therefore, security protocols based on international standards must be implemented in public administrations. The information concerning the detection of weaknesses and risks in the ADMGEC Data Center is guided by the technical evaluation to specify compliance according to ISO / IEC 27002 and ICREA 2013 standards and will be carried out through in-depth interviews with the technical maintenance staff of ADMGEC Systems, which are directly related to this infrastructure, with the purpose of knowing how the data center is managed, observing the continuous improvement of security.

KEY WORDS: DATA CENTER, ADMGEC, TECHNOLOGICAL RISK, STANDARDS.

INTRODUCCIÓN

1.1 Presentación de la investigación

El presente trabajo de investigación parte del estudio del sistema, herramientas informáticas y técnicas de seguridad organizacionales que forman parte de la infraestructura del Centro de Datos del Gobierno Autónomo Descentralizado Municipal del Cantón de Esmeraldas (GADMCE), con la finalidad de detectar las debilidades y necesidades existentes y en base a ello, formular una propuesta de mejora.

1.2 Planteamiento del problema

El GADMCE es una entidad de Derecho Público, cuya finalidad es servir a la comunidad, manejando información de mucha importancia; cuenta con un sistema informático que en el transcurso de los años ha incrementado progresivamente la cantidad de información almacenada, así como la incorporación de nuevos usuarios relacionados con el área administrativa y la comunidad en general. Esto hace necesario establecer condiciones adecuadas para procesar la información mediante un Plan de Seguridad Informática.

Es relevante tener presente que la Informática es una de los puntales principales de las instituciones, sean públicas o privadas, siendo que manejan información la cual se sube a una plataforma informática, llevándose a cabo actividades de servicio, comerciales, comunicaciones.

El GADMCE siendo una entidad pública debe contar con una planificación orientada a la protección de la información y prevención de riesgos tecnológicos, debido a la incidencia de casos graves, que impedirían el restablecimiento de operaciones en tiempo prudencial.

El GADMCE no cuenta con manejo de procedimiento de seguridad en el Centro de Datos y no tiene la documentación debida, trabaja bajo lineamientos informales, exponiendo la seguridad de la información y da cabida a la fuga de información o eventualidad que se encuentra fuera del control establecido, afectando el normal funcionamiento de los servicios de TI implementado en la infraestructura del centro de datos.

Los controles de accesos a cuentas del personal administrativo para ingreso a los sistemas, equipos y servicios, son poco eficientes debido a la falta de normativa en el proceso. Lo correcto es la existencia de un registro de acceso y monitoreo continuo del mismo. De presentarse un incidente que afecte a la seguridad de la infraestructura tecnológica (sea por factor lógico, físico o humano) podría ocasionar graves consecuencias en el funcionamiento de una entidad pública, por lo que es importante tomar decisiones que permitan facilitar la administración de riesgos en base la normativa internacional.

La pérdida de la información almacenada ocasionaría un caos, consecuencias graves en una entidad, por lo que es importante realizar toma de decisiones que permita facilitar la administración de riesgos. Por ello, el desarrollo del proyecto está sustentado en el estudio y formulación de un modelo de técnicas de seguridad organizacional y herramientas informáticas para la infraestructura del Centro de Datos del GADMCE, con la finalidad de detectar las debilidades y necesidades existentes con respecto la seguridad informática. Es elemental mantener controles de seguridad los cuales colocan en buen recaudo la información que se encuentra en los Centros de Datos.

Desde ahí nacen interrogantes como: ¿Cuál es el nivel de seguridad del centro de datos? ¿Qué normas de seguridad analiza los riesgos de la infraestructura?

1.3 Justificación del estudio

El centro de datos del GADMCE tiene como objetivo el crecimiento ordenado de toda su infraestructura tecnológica, seguridad física, respaldo de información, uso de energía

eficiente y confiable, adaptabilidad en los equipos, todo esto en condiciones de climatización establecidas por las condiciones de garantía de los fabricantes de los equipos para buen funcionamiento, uso y conectividad, considerando la integración de las diferentes plataformas y dependencias de la institución. La misma brinda servicios considerados críticos y de vital importancia, tanto para usuarios externos, ciudadanía de Esmeraldas, como para el personal administrativo perteneciente a la Municipalidad.

En el centro de datos del GADMCE se encuentra varias tecnologías, con la finalidad de brindar servicios de relevante importancia a la comunidad de la ciudad de Esmeraldas, asimismo considerando a los usuarios de los diferentes departamentos que lo conforman.
El GADMCE al transcurrir los años ha ido incrementando sistemas tecnológicos, que facilitan el cumplimiento de pagos de las obligaciones de la ciudadanía, calidad de servicio que se mantiene por todos los días del año.

La Unidad de Sistemas del GADMCE realizó modificaciones en el cableado estructural debido a la separación de los departamentos municipales a diferentes edificaciones por la emergencia generada por el terremoto del año 2016 y sus posteriores réplicas. La operación demandó mayor esfuerzo del personal de la unidad para restablecer los servicios y operar bajo óptimas condiciones. A pesar de la medida tomada, no se contempló un plan de riesgos sino que se actuó con conocimientos en base al sentido común, exponiendo al activo del centro de datos a riesgos tecnológicos latentes.

El GADMCE se beneficiaría de la propuesta del análisis de los riesgos tecnológicos del Centro de Datos porque en base a los resultados obtenidos se especificarán las debilidades del sistema informático y por medio de recomendaciones, aplicar correctivos, establecer políticas, procesos y controles de seguridad amparándose en las normativas internacionales.

1.4 Objetivos

Objetivo General

Aplicar una evaluación de seguridad de la infraestructura tecnológica del centro de datos del GADMCE a través de las normas ISO 27002 e ICREA STD 131-22013 para establecer alternativas de mitigación.

Objetivo Específicos

- Identificar las normas ISO 27002 e ICREA STD 131-22013.
- Analizar la infraestructura tecnológica del Centro de Datos del GADMCE.
- Determinar el nivel de riesgo informática aplicando las normas ISO 27002 e ICREA STD 131-22013 para el análisis de riesgos en infraestructura tecnológica.
- Realizar un informe ejecutivo de la evaluación técnica donde se evidencia los hallazgos, observaciones y recomendaciones.

CAPITULO I: MARCO DE REFERENCIA

1.4.1. Antecedentes (Estudios previos)

Para el desarrollo de este plan se consideraron algunas investigaciones que sirvieron de guía para la realización de esta investigación y se describen a continuación.

En la investigación titulada "Proveer criterios y directrices para diseñar, construir e implementar el Centro de datos para el GAD de Loja, basada en la norma internacional ICREA-Std-131-2013 con aplicabilidad a normas y regulaciones nacionales" ayuda como guía para lograr mitigar vulnerabilidades y riesgos utilizando la normativa ICREA-Std-131-2013 en el caso GAD de Esmeraldas (Guamán Carrión, 2015)

Por otro lado, el artículo titulado "Riesgo y vulnerabilidades para los centros de datos de México y América Latina", enfatiza que según la International Computer Room Experts Association (ICREA), estándar internacional que regula la formación, construcción, gestión, mantenimiento, los niveles de seguridad y la sustentabilidad de los centros de datos; donde el principal riesgo de seguridad es el error humano, el cual puede ser involuntario. No obstante, ese error a veces es doloso. Al realizar el análisis del criterio es importante resaltar que el uso de esta norma hará que el personal encargado del mantenimiento de la infraestructura, realice una muy acertada toma de las medidas pertinentes.

Una empresa en el Ecuador se ha certificado con las normas ISO 27001, es la empresa Corporación Nacional de Telecomunicaciones CNT EP, la cual recibió la certificación el 29 de mayo del 2015 "Sistema de Gestión de la Información bajo la norma ISO 27001 SGSI" por parte de la Asociación Española de Normalización y Certificación AENOR (Ecuador). Esta certificación no solo busca la calidad, sino que se preocupan por la seguridad en la información que se maneja (CNT Sala de Prensa, 2015)

En la Conferencia Cisco 2016 en el Informe Anual de Seguridad, realizado en el verano del 2015 y que incluyó a 12 países (entre los cuales no está Ecuador) en uno de sus

puntos tratados menciona a la Infraestructura vulnerable y rápidamente explotada, donde los atacantes están aprovechando recursos legítimos, convirtiéndose en expertos para desplegar campañas difíciles de detectar. Esto alienta a la realización del estudio considerando que se debe tomar las medidas pertinentes con respecto a los procesos correspondientes para la gestión de seguridad de la infraestructura del centro de datos del GADMCE. (Fernandez, 2016).

Entre las notas encontradas, en la sala de prensa "Valdez Albizu informa Banco Central obtiene certificación ISO 27001" se informa que el Banco Central de la República Dominicana obtiene la Certificación ISO 27001, luego de realizar la auditoria final y confirmar que cumple con todos los requisitos de seguridad de información. Como antecedente, tiene implementado la gestión integral de riesgo y continuidad del negocio basado en la Norma ISO 31000, Basilea II, el Estándar BS 25999, ITIL y demás estándares, con la finalidad de cumplir con los principios de buenas prácticas de gestión de aceptación mundial. Por ende, lograr la certificación ISO 27001 corresponde otro peldaño en su paso a la excelencia empresarial. Para la realización del proyecto se extrae la importancia de la aplicación de normas internacionales en agencias gubernamental, justificando de ese modo el desarrollo del tema. (Valdez, 2013)

1.4.2. Bases teóricas científicas

1.4.2.1. Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas

Los gobiernos autónomos descentralizados municipales son personas jurídicas de derecho público, que cumplen competencias exclusivas que ayudan a la ciudadanía del cantón. (Dirección de Comunicación del Ministerio de Coordinación de la Política y Gobiernos Autónomos Descentralizados, 2011)

El GADMCE pertenece a la Asociación de Municipalidades Ecuatorianas (AME) y como todos los gobiernos autónomos descentralizados municipales del Ecuador, es considerada persona jurídica de derecho público, que cumple competencias exclusivas que ayuda a la ciudadanía del cantón. (Dirección de Comunicación del Ministerio de Coordinación de la Política y Gobiernos Autónomos Descentralizados, 2011). Está

conformado por departamentos, donde la principal autoridad es el señor Alcalde seguido de la Vice Alcaldesa y con el apoyo del Concejo Cantonal.

1.4.2.2. Infraestructura de TI

1.4.2.2.1. Ubicación

Dentro de los diferentes departamentos y servicios en los que se desglosa el Municipio de Esmeraldas se encuentra la Jefatura de Sistemas, que forma parte de la Dirección Administrativa.

En la **Figura 1** se observa su ubicación en el organigrama del GADMCE.

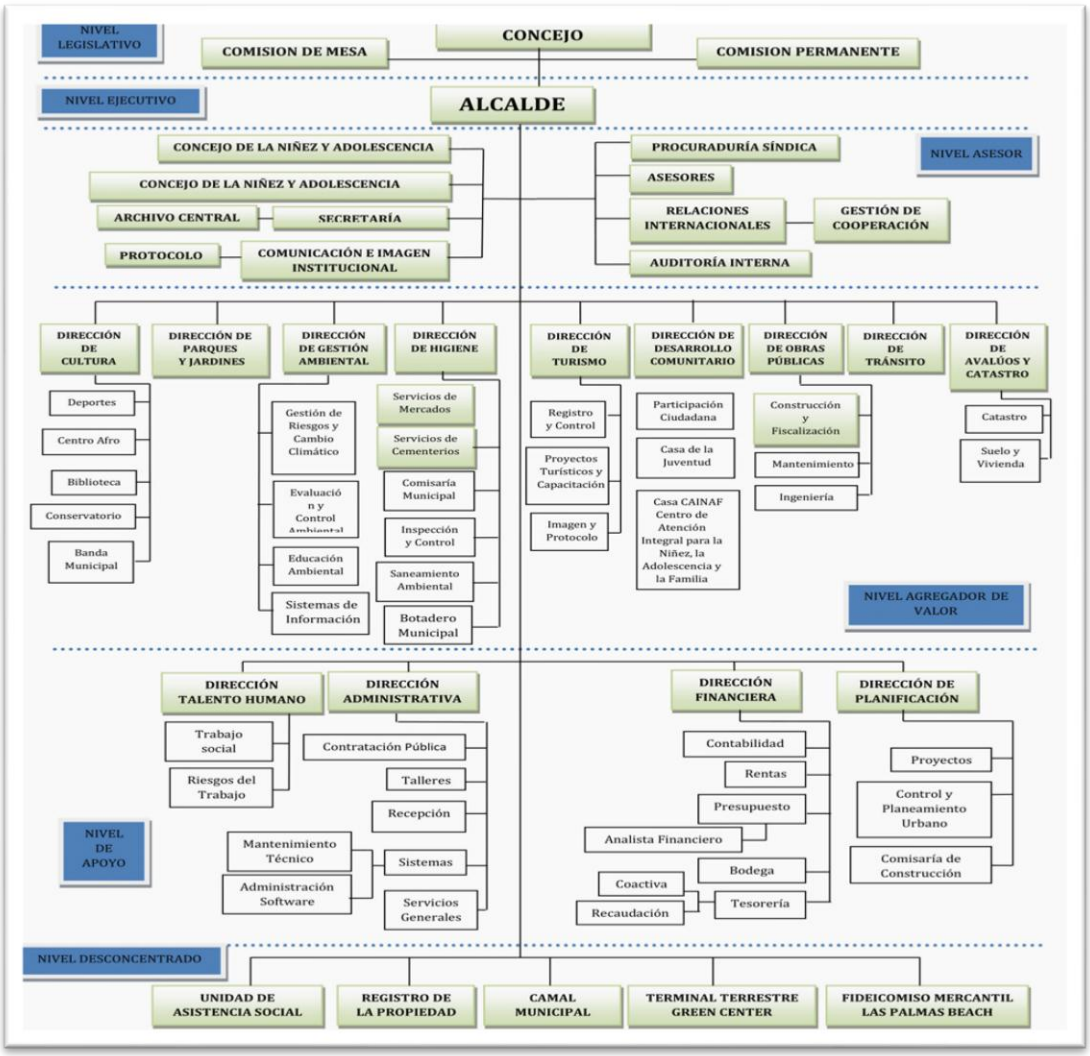


Figura 3. Orgánico Estructural GADMCE (MUNICIPIO-ESMERALDAS, 2016)

1.4.2.2.2. Unidad de Sistema

La Unidad de Sistema del GADMCE es la que administra eficientemente los recursos informáticos, mediante la utilización de tecnologías de la información y la automatización de procesos, con la finalidad de apoyar de manera eficaz la gestión y la toma de decisiones administrativas en beneficio de la colectividad. En la **figura 2**, se aprecia como la Unidad de sistema del GADMCE se encuentra organizada:

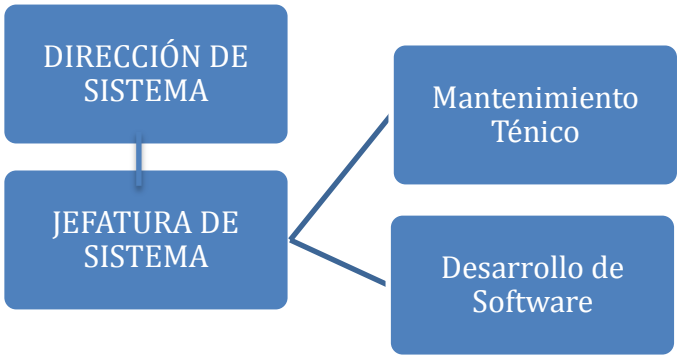


Figura 4. Estructura de Unidad de Sistema

Fuente: Proporcionada por Jefe de Sistema del GADMCE

El área del Mantenimiento Técnico está basada en controlar, vigilar el buen estado de las redes y buen funcionamiento de todos los equipos informáticos existentes; y en especial salvaguardar el estado físico de los servidores, dispositivos de comunicaciones de voz y datos. El personal especializado en proteger los activos de información hospedados en el centro de datos, administra la infraestructura, con el fin de cumplir con tareas de mantenimiento, control, desarrollo del cableado estructurado y servicios de red.

A continuación se detalla en la **tabla 1** los componentes seleccionados de la infraestructura tecnológica de la empresa, en la que se incluye las especificaciones de todos los activos. La institución consta servidores, tiene equipos de escritorio y portátiles distribuidos de la siguiente forma:

Tabla 1. Dispositivos de Infraestructura de TI del GADMCE (GADMCE, 2017)

EQUIPO	MARCA	CAPACIDAD	MEMORIA	PROCESADOR	AREA
Servidor de Internet	HP Proliant DL380 G6	2 TERA	16 GB	Intel xeon	Sistemas
Servidor	HP Proliant DL360P G8	4 TERA	16 GB	Intel xeon	Sistemas
30 Computadoras	HP	1 TERA	8GB	Intel core i7	Catastro
Servidor	HP Proliant DL160 G6	500GB	8GB	Intel Xeon	Sistemas
19 Computadoras	HP	1 TERA	8GB	Intel core i7	Planificación
Servidor	HP Proliant DL380 G6	1 TERA	8 GB	Intel xeon	Sistemas
Servidor	HP X1400	1 TERA	4GB	Intel Xeon	Sistemas
8 Computadoras	HP	1 TERA	8GB	Intel core i7	Sistemas
1 Computador	HP	1 TERA	8GB	Intel core i7	Tesorería
1 Computador	COLOR SIT	1 TERA	8GB	Intel core i7	Transito

2 Computadoras	HP	1 TERA	8GB	Intel core i7	Rentas
1 Computador	QUASAD	1 TERA	8GB	Intel core i7	Contabilidad
EQUIPOS DE REDES					
SWITCH			D-LINK, 8 PUERTOS		
ROUTER			D-LINK, 15		
CAMARAS DE VIDEO VIGILANCIA			5		
LINEA DE ACCESO A INTERNET			CNT		

1.4.2.2.3. Diagnóstico de Seguridad Física y Lógica

En lo que se refiere a seguridad física de la entidad, cuenta con un personal de guardia, debido a esto no cualquier persona puede acceder a las instalaciones del GADMCE.

El acceso de la oficina es controlado, el espacio estimado área de TI cuenta con un ambiente de ventilación básica. Existe personal autorizado para el manejo de los equipos, además para poder acceder al servidor se tiene restricciones, el acceso lógico de seguridad el cual exige un usuario con su respectiva contraseña de acceso.

Se realiza registro a través de la bitácora identificando el nombre completo del usuario, fecha y hora de entrada y salida, actividad realizada. En caso de ingresar un visitante debe identificarse con el gafete respectivo en compañía del responsable autorizado.

Existe UPS con la finalidad de prevenir descargas eléctricas, activándose inmediatamente en el intervalo de tiempo la acción de salvaguardar información y tiene un lapso de tiempo de energía de 30 minutos.

1.4.2.2.4. Redes y comunicaciones

El espacio destinado como área de TI, posee un nivel de seguridad física debido a que se encuentra en un área departamental, existe estantería para el posicionamiento de los equipos de comunicación.

El área tiene 5 servidores en el cual se almacena y administra el sistema de información además del manejo de backups de la institución, donde el encargado de TI realiza el control de accesos de usuarios y contraseñas.

El router tiene conexión inalámbrica, uno de los portátiles está a más de 200 metros de distancia del router para cubrir dicha distancia, se coloca un punto de extensión de esa manera todos los dispositivos inalámbricos salir a Internet.

1.4.2.2.5. Software

En la actualidad la institución utiliza el sistema CABILDO y SIGAME, los mismos que se encargan de manejar y almacenar la información de mucha importancia, como la parte contable y financiera de la institución, así como también la parte catastral actualizada.

El formato del correo electrónico institucional es :
nombreUsuario.apellidoUsuario@esmeraldas.gob.ec

1.4.2.2.6. Servicio Web e Internet

El servicio del Internet que posee la institución es proporcionado por un plan corporativo de CNT contratado de 30 megas implementado en cada uno de los departamentos, actualmente de conexiones de radios con los demás edificios donde funcionan las diferentes dependencias del GADMCE.

El sitio Web da a conocer Ley de Transparencia, PAC, POA, Resoluciones, consultas de impuestos prediales, guías de trámites entre otras. Hay momentos que se dan obligados en interrumpir sus funciones debido a la caída del servicio del Internet, por existir problemas con el proveedor en cumplir su funcionabilidad, ocasionando la inconformidad y descontento tanto para el personal que labora en la institución como al usuario que es parte de la ciudadanía.

1.4.2.2.7. Topología de Red

El GADMCE cuenta con una distribución de conexiones de red que está conformado por 15 router y 12 swicht como se puede identificar en la Figura 3.

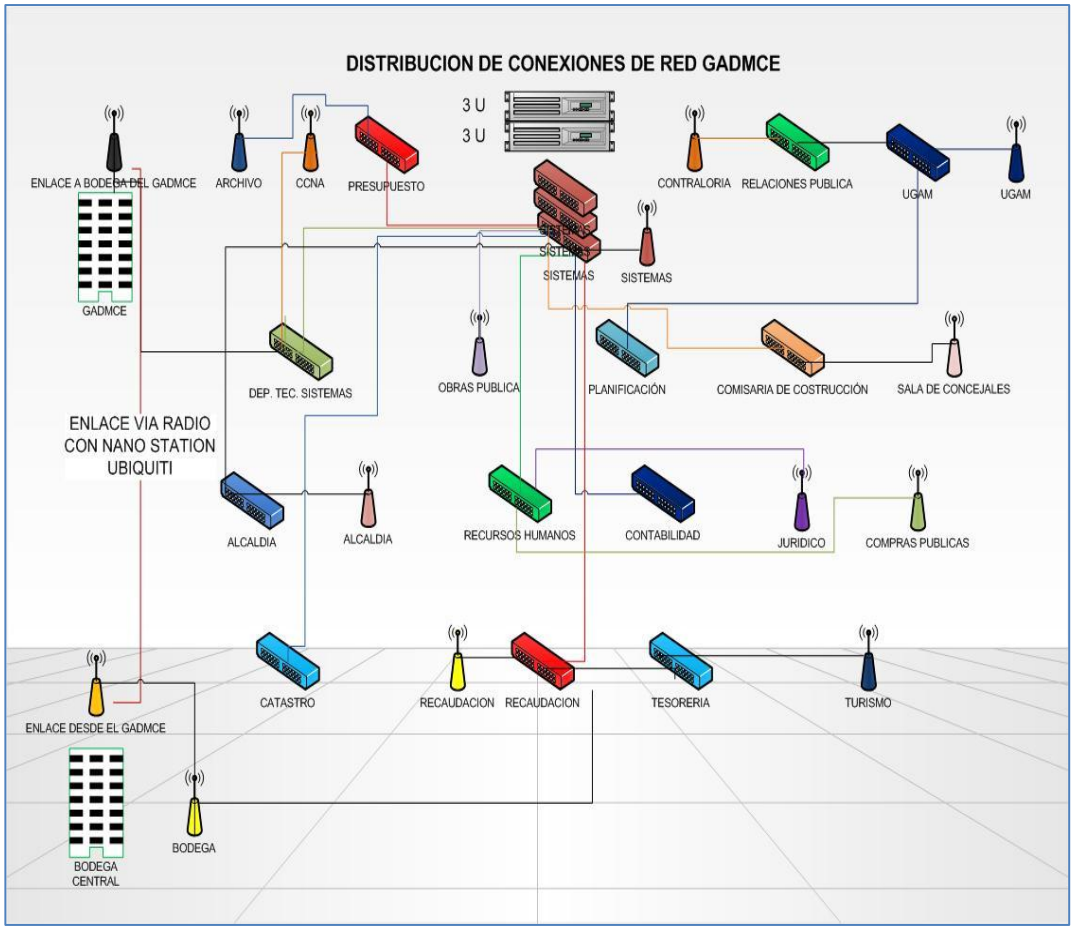


Figura 3. Topología de Red GADMCE. (Mosquera, 2017)

1.4.2.2.8. Detección de problemas de infraestructura

Existe una buena asignación de funciones a cada personal encargado del área de TI, ocasiona una eficiencia en el servicio de soporte a usuarios, en el manejo adecuado de la seguridad física y lógica tanto de la información como de la infraestructura.
El Sistema Operativo de los equipos en su mayoría se encuentra debidamente licenciado.

El espacio asignado a la infraestructura debe llegar a cumplir con las exigencias de adecuación para la misma, el ambiente no es fresco por lo cual los equipos están expuestos a sobrecarga, falta de planta de emergencia, no posee piso falso.

1.4.2.3. RIESGO TECNOLÓGICO

La pérdida importante por daño, interrupción o fallas derivadas del uso de hardware, software, redes y otro canal de distribución de la información de una institución se comprende como riesgo tecnológico. Las fallas en la infraestructura de TI representan pérdidas financieras, acrecentando las consecuencias de eventos adversos.

Tipos

El riesgo tecnológico se presenta en los tres niveles de una organización que cuenta con apoyo de las Tecnologías de la Información (Ortiz, 2013):

- Infraestructura tecnológica: riesgo asociado con hardware.
- Lógico: comprende a las posibles eventualidades que afecten al software.
- Recurso humano: cuando el riesgo en la infraestructura tecnológica o a nivel lógico se materializa debido a la incorrecta manipulación.

Características

El riesgo tecnológico implica (Peña, 2010):

- Probables perdidas ante fallas de sistemas de información.
- Probabilidad de fraudes, externos e internos, mediante el empleo de los sistemas de información.
- Conlleva a riesgo legal y perjuicio en la reputación de la organización debido a fallas en la seguridad y no disponibilidad de los sistemas de información

1.4.2.4. NORMAS INTERNACIONALES SOBRE RIESGO TECNOLÓGICO

ISO 31000

Por medio de la implementación de la norma ISO 31000, las organizaciones pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente. La norma gestiona sus riesgos en forma eficaz tiene más contingencias de protegerse y obtener éxito en los procesos de una organización para llegar a formar parte de la toma de decisiones de manera dinámica y sensible al cambio, facilitando así la mejora continua en el crecimiento de sus negocios.

ICREA

El ICREA "International Computer Room Expert Association", se encuentra formada por ingenieros/as especializados/as en el diseño, construcción, mantenimiento, adquisición instalada y auditoría de centros de cómputos. Es el único organismo que norma y certifica productos de Infraestructura TIC.

El análisis que estime las prioridades de riesgo sería necesario al construir un centro de cómputo con la finalidad de protegerlo, considerando el personal de operación, las normas de seguridad, su entrenamiento y construcción aplicable, las especificaciones de los fabricantes, los procedimientos utilizados para la conservación de equipos, la redundancia deseada y procedimientos de recuperación en caso de daños en la infraestructura.

Considerando como equipo de cómputo, a todos los equipos electrónicos de proceso que estén vinculados a una misma red de comunicación de datos, al momento de considerarse un lugar, se debe evaluar el punto de seguridad, la alimentación eléctrica, las vibraciones, posibles problemas estructurales e inundaciones.

ISO/EC 27001

El sistema de Gestión de Seguridad de la Información SGSI), se basa en la norma ISO/EC 27001, la cual ha sido elaborada bajo los procesos de planificar- hacer- verificar- actuar (PHVA).

Este modelo fue concebido con la finalidad de aplicar a toda empresa e instituciones, tanto públicas como privadas, y se debe determinar continuamente el mejoramiento, y su debida documentación la cual registrarán el plan de actividades, detallando las actividades y operaciones que se realicen.

1.4.2.5. Análisis de riesgo tecnológico

Para la realización de análisis de riesgos a una estructura tecnológica, es necesario basarse en normativa para avalar que los resultados se obtuvieron de manera consensuada y que las mejoras propuestas tienen un motivo. Las normas internacionales ICREA 2013 e ISO 27002 brindan un soporte de confiabilidad para las instituciones, sean públicas o privadas, para realizar sus actividades sabiendo que están amparados en caso de sufrir interrupciones de servicios.

El análisis que estime las prioridades de riesgo sería necesario al construir un centro de cómputo con la finalidad de protegerlo, considerando las exigencias de la norma internacional ICREA 2013, como es: el personal de operación, las normas de seguridad, su entrenamiento y construcción aplicable, las especificaciones de los fabricantes, los procedimientos utilizados para la conservación de equipos, la redundancia deseada y procedimientos de recuperación en caso de daños en la infraestructura. (Guamán Carrión, 2015)

Además, resultan necesario los procesos metodológicos estandarizados como ISO/IEC 27002 para el diseño de estrategia para la seguridad informática. Es moderno y tiene extensa aceptación mundial para la construcción de la seguridad organizativa. (AENOR, 2012)

Al establecer el Sistema de Gestión de Seguridad de la Información (SGSI), la organización debe concretar el alcance y los límites, bajo los términos de negocio, política de la organización y precisar procedimiento para identificación, evaluación y posterior mitigación del riesgo, observando el impacto que el riesgo puede ocasionar sino se posee un mecanismo de implantación de controles. En la organización es vital tener un plan de tratamiento de riesgo, puntualizar el proceso de implantación para el plan de tratamiento de riesgo e implantación de los controles para posteriormente medir si se lograron cumplir con los resultados.

Es relevante que se cumpla con los requerimientos de documentación para ser monitoreadas, con el fin de realizar la evaluación de su efectividad. Debe ser registrados los siguientes documentos (iso27000.es, 2012):

1. Declaración de la política y objetivos de control.
2. El alcance del SGSI.
3. Los procedimientos y controles que dan soporte al SGSI.
4. Una descripción de la política de valoración de riesgo.
5. La valoración del informe de riesgo
6. El plan de tratamiento de riesgos.
7. Los procedimientos documentados necesarios para que la organización se asegure la planificación efectiva.
8. La declaración de aplicabilidad.

La documentación debe ser manejada con eficiencia, protegerla de manipulaciones, con la finalidad de mantener la integridad del control de registros existentes, como son el registro de visitantes, registro de auditoria y solicitudes de acceso legibles. Es relevante que las personas asignadas se le establezcan roles y responsabilidades, y asimismo sea abastecido de los suministros de manera efectiva y enfatizando que el criterio de nivel de riesgo sea aceptable para la institución.

La siguiente norma de la familia de la ISO 27000 es utilizada para el análisis de riesgos es la ISO/IEC 27002. Es una “norma contiene 14 dominios, 35 objetivos de control y 114 controles”, y es considerada una herramienta que permite organiza políticas y

controles con el objetivo de reducir los riesgos informáticos en la Institución. (Consultor, 2013)

No solo se refiere a las áreas de tecnología de la información, también orienta en asuntos organizacionales, seguridad física, administración de políticas, gestión de personal, entre otros mediante la aplicación de controles.

Con la existencia de riesgos tecnológicos, es necesario la garantía de que los servicios críticos no sean interrumpidos durante alguna situación adversa. Con la finalidad de prevenir situaciones que paralicen las actividades normales se ha incrementado la continuidad del negocio en caso que: no se cuenta con el personal idóneo, perdida de información magnética, destrucción y daños en las instalaciones causados por desastres naturales y falta de energía eléctrica.

En las instituciones, es necesario aplicar controles de tipo administrativo con respecto a ambientes de procesamientos automáticos de datos. De este modo, se valora el control interno y su incidencia tanto administrativa como financiera, con la finalidad de diagnosticar el estado actual mediante un informe de control interno el cual está sujeto a verificaciones de cumplimiento de optimización del desarrollo de procedimientos con la finalidad de detectar las debilidades existentes para ser analizados y corregidos (Heredia, 2015).

Ahora, para el desarrollo de proceso análisis y gestión de riesgos de un sistema informático se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización.

Los recursos son los activos a resguardar del sistema informático de la organización. Una amenaza puede ser cualquier evento accidental o intencionado que pueda afectar al sistema informático, provocando pérdidas materiales y financieras; causando daños secuenciales.

Para la medición se establece el término impacto, que representa a la valoración del daño que podría producir a la organización un incidente de seguridad. Para eliminar o reducir el riesgo es necesario aplicar herramientas salvaguardas. En otras palabras, objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización. (Miler, M., 2008)

Para el centro de datos, se tendrá que disponer de una sala fundamentalmente acondicionada para ubicar los servidores centrales con todos los ficheros y aplicaciones informáticas de modo que se pueda controlar el acceso físico de personal especializado relacionado con el sistema informático (Fine, Seguridad en centros de cómputo, 2002).

1.4.1.5. Análisis y Gestión de Riesgo en un sistema informático

En el desarrollo de proceso de gestión se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización.

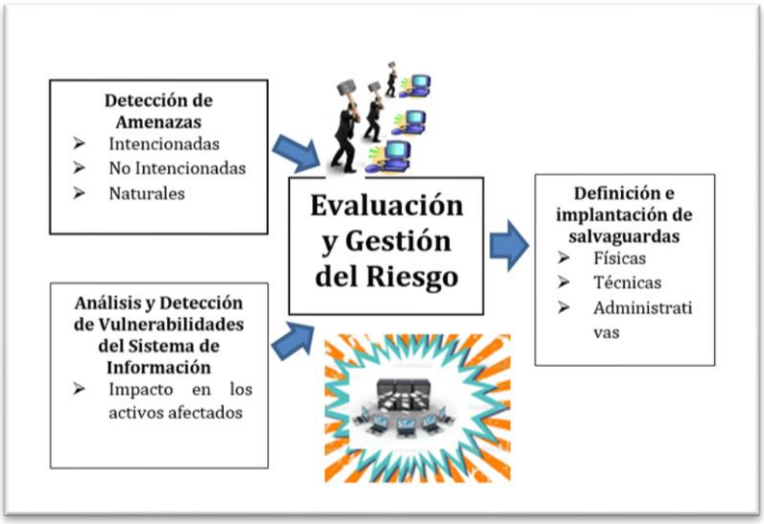


Figura 4. Análisis y gestión de Riesgos en una organización (Gómez V., 2011)

Los recursos son los activos a resguardar del sistema informático de la organización. Una amenaza puede ser cualquier evento accidental o intencionado que pueda afectar al sistema informático, provocando pérdidas materiales y financieras; causando daños secuenciales.

El impacto es la medición y valoración del daño que podría producir a la organización un incidente de seguridad, por medio de salvaguardas o medida de seguridad es cualquier medico empleado para eliminar o reducir u riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización. (Miler, M., 2008)

1.4.3. Marco Legal

La Contraloría General del Estado en el Registro Oficial No. 78 del martes 1 de diciembre de 2009, bajo la Administración del Señor Ec. Rafael Correa Delgado, Presidente Constitucional de la República del Ecuador emite las Normas de Control Interno para las Entidades, Organismos de Sector Público y personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos en el Código 410-10, con descripción de Seguridad de Tecnología de Información; indicando los mecanismos y medidas que se establecerá para la protección y seguridad de la información, así como proteger la infraestructura. (Registro Oficial No. 78, 2009). El GADMCE como entidad que tiene a su disposición recursos públicos y maneja información sensible de los ciudadanos esmeraldeños debe cumplir con lo estipulado en el Código 410-10.

Mediante Acuerdo Ministerial 166 Suplemento 88, la Secretaría Nacional de la Administración Pública implantó la Comisión para Seguridad Informática y Comunicación, la cual dentro de sus atribuciones tiene la de crear lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado a ésta para las entidades de la Administración Pública Central e Institucional. Debido a los denominados ataques informáticos o cibernéticos, la Administración Pública debe actuar de forma integral y coordinada para minimizar o anular riesgos en la información, así como también proteger la infraestructura. (Castillo, 2013)

En el Código Orgánico Integral Penal Suplemento 180, publicado el 10 de febrero de 2014, establece en el artículo 233 de Delitos contra la información pública reservada legalmente, establece que: "la persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años" (Código Orgánico Integral Penal Suplemento N°180, 2014). Si durante el proceso de auditoria se llega a descubrir irregularidades con respecto a manipulación de información reservada, el GADMCE tiene la obligación de acusar amparándose en el artículo mencionado.

CAPITULO II: MATERIALES Y MÉTODOS

2.1. Descripción del lugar

2.1.1. Ubicación

País: Ecuador

Provincia: Esmeraldas, Distrito Centro, Av. Simón Bolívar 9 de Octubre.

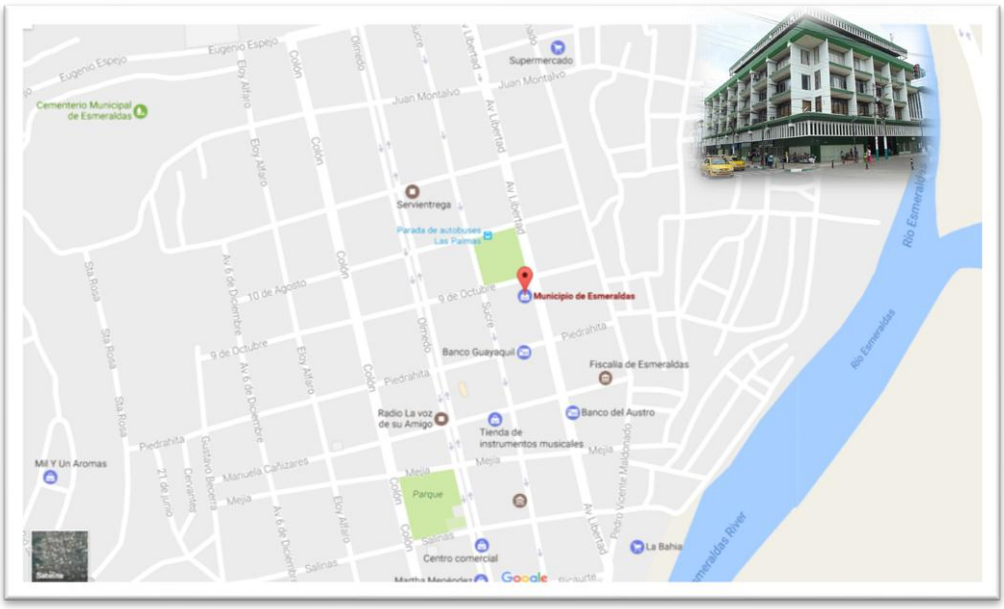


Figura 5. Ubicación geográfica del GADMCE *(GAD de Esmeraldas, 2016)*

2.2. Métodos y técnicas

El diseño de esta investigación estuvo basado en la metodología tecnológica aplicada, es decir que busca trasformar la realidad del objeto de estudio; usando estándares y normas internacionales de seguridad de la información digital que ayudará a la obtención de un buen diagnóstico de la seguridad del Centro de Datos. Esta metodología tiene por finalidad reconstruir procesos en función de indagaciones previas (Bello, 2013).

En esta investigación se aplica el método cualitativo, debido al estudio de la realidad en su contexto natural, intentando sacar la interpretación de los fenómenos de acuerdo con

los significados que tienen para las personas implicadas. La investigación cualitativa implica la utilización y recogida de una gran variedad de materiales, sea entrevista, experiencia personal, imágenes, sonidos que describen la rutina y las situaciones del problema y significado (Rodríguez, Gil, & Garcia, 1996).

Se elige este método porque es necesario contar con interpretación de resultados y en base a ello, proceder al planteamiento de la propuesta. En la investigación se buscó conocer la situación del Centro de Datos del GADMCE y contrastar de qué manera se puede hacer frente a los riesgos tecnológicos. Luego se analiza la importancia de aplicar las normas para contrarrestar los riesgos en la infraestructura de TI de la institución.

2.3. Población

En 2016, el GADMCE contó con una Unidad de Sistemas integrada por diez profesionales: el Jefe de la Unidad, cuatro desarrolladores de software y cinco de soporte técnico. Para la realización de las entrevistas necesarias se considera al Jefe de la Unidad, Encargado del Centro de Datos, Jefe de Desarrollo de Software, Jefe de Soporte Técnico.

La población de estudio, por tanto, la constituyen las 4 personas, por ser quienes directamente tienen funciones relacionadas con la preservación de la seguridad del Centro de Datos del GADMCE y la reducción de riesgos. A pesar que la población es menor de 30, no es necesario trabajar con todos ellos. A los mencionados se le realiza la entrevista con el fin de obtener información relevante respecto a servicio críticos, las políticas de administración, vulnerabilidades más notorias, los recursos más utilizados y las necesidades de capacitación del personal.

2.4. Técnicas de procesamiento y análisis de datos

Se realizó entrevistas al personal de la Unidad de Sistemas calificado ayudándose de una grabadora y de la guía de preguntas necesarias para la entrevistas con la finalidad de obtener la información necesaria para el proyecto. Además, se utilizó una matriz para la auditoria en la que constan los criterios que establece la norma ICREA 2013 para

inspeccionar el centro de datos y determinar en porcentaje el nivel de desarrollo que tiene la infraestructura tecnológica en los diferentes aspectos, como son: obra civil, climatización, comunicaciones, electricidad y seguridad. También se aplicó la metodología planteada por la ISO 27002 para análisis de riesgo tecnológico a los elementos que constituyen el centro de datos como son componentes eléctricos, cableado estructurado, servidores, entre otros. Se tomó fotos como constancia de lo observado valiéndose de un teléfono inteligente.

Para el análisis de los resultados de las entrevistas, dividió en cuatro partes: análisis de la entrevista al Jefe de sistemas, al Encargado del Centro de datos, al Jefe de Desarrollo de Software y por último, la entrevista realizada al Jefe de Mantenimiento Técnico.

Se hizo un análisis general con la finalidad de obtener información del tema en estudio.

2.5. Normas éticas

Se precisó información real para el desarrollo del plan, con la finalidad de tomar decisiones en base a resultados obtenidos, lo cual benefició la manera de administrar el Centro de Datos del GADMCE.

El discernimiento emitido en el desarrollo de esta investigación es exclusivamente del autor, por ende, los artículos y demás datos mencionados en el contenido del estudio que se relacionan con el Análisis de Riesgo Tecnológico del Centro del GADMCE, están citados según los criterio de las normas APA sexta edición, observando los autores y años de publicación. Los nombres de las personas entrevistadas no serán mostrados, se limita a indicar el cargo.

CAPÍTULO III: RESULTADOS

3.1. Análisis e interpretación de resultados

Análisis de la entrevista realizada al Jefe de la Unidad de Sistemas.

La Jefatura de Sistemas debería implementar un Plan Operativo formal y considerar la estructuración de un Plan Estratégico de TI. Además, deben definir más procesos administrativos pertenecientes al Centro de Datos. Es necesaria la planificación para hacer frente a riesgos tecnológicos latentes.

Análisis de la entrevista realizada al Administrador de Centro de Datos.

El profesional indica la problemática generada por el desastre natural suscitado el 16 de Abril del 2016 y la solución plateada se está gestionando. Pero, declara la ausencia de un pilar fundamental en una infraestructura tecnológica, la estandarización. Si bien es cierto que el centro de datos opera dentro de lo aceptable, es necesaria la regularización para optimizar recursos. Respecto al tratamiento de riesgo, no especifica si el respaldo se encuentra en la nube de cómputo o físico. Tampoco mencionada las medidas a tomar respecto a ataques informáticos.

Análisis de la entrevista realizada al Jefe de Mantenimiento Técnico.

El entrevistado hace notar que, a pesar de contar con los sistemas necesarios para garantizar los servicios en la institución, la carencia en la estructura del centro de datos es notable. Indica la falta de servidores, que impiden la normalidad en las actividades. El profesional reconoce que es necesaria la adquisición de equipos servidores para respaldar la información y no depender de un sistema de espera que representa retrasos en las actividades. Además, La falta de un generador eléctrico expone de manera negativa la continuidad de los servicios. El GADMCE tiene actividades importantes para la ciudadanía, maneja datos que deben estar disponibles siempre que se los requiera debido a que no puede paralizarse el trabajo por la falta de energía eléctrica.

Análisis de la entrevista realizada al Jefe de Desarrollo de Software.

El entrevistado recalca la falta de un sistema de la red eléctrica completa. El principal problema que tiene el centro de datos es la interrupción de energía eléctrica. El encargado de Desarrollo de Software hace notar que la información de la institución se encuentra en riesgo por no garantizar su integridad debido al caso que expone, no almacenar a tiempo las modificaciones correspondientes a las estructuras de la base de datos.

CAPÍTULO IV: PROPUESTA DE INTERVENCIÓN

4.1. Análisis de Riesgo Tecnológico del Centro de Datos del GADMCE basado en normas internacionales.

Para proceder con el análisis de riesgo, fue necesaria una auditoria al centro de datos del GADMCE del 10 de abril del 2017 al 14 de abril del 2017. Se tiene como consigna emitir una opinión respecto a los controles de la infraestructura tecnológica en estudio usando las herramientas planteadas para el proyecto.

El análisis de riesgo se elaboró con los lineamientos de la norma ICREA 2013 y el estándar ISO/IEC 27002. La normativa indicada requiere de planificación con la intención de alcanzar un aceptable grado de seguridad. Entre las actividades realizadas fueron: inspección del espacio físico del centro de datos, recolección de evidencias de observación, políticas y evaluación de procedimientos de control practicados por los profesionales a cargo. La información conseguida constituye una base fundamental para la obtención de conclusiones.

El análisis de riesgo tecnológico es una evaluación que se realiza a los controles que se emplean para garantizar la protección ante amenazas y vulnerabilidades.

En primera instancia, fue necesaria la identificación de los activos pertenecientes al centro de datos sometido a estudio. Estos activos influyen de manera directa en la confidencialidad, integridad y disponibilidad de la información en la entidad. Haciendo uso de la Norma ICREA 2013, se elabora un cuadro donde constan todos los ámbitos necesarios en una infraestructura tecnológica.

Tabla 2. Aplicación de la Norma ICREA 2013 en el GADMCE *(Onofre, 2015)*

ÍTEMS	Cumplimiento	
	SI	NO
Instalaciones Eléctricas		
Energía eléctrica con alimentadores independientes de otras cargas	X	
Sistemas de puesta a tierra aislada	X	

Sistemas de puestas a tierra de seguridad		X
Interconexión entre los diferentes sistemas de puesta a tierra	X	
Supresión de transistores de sobre tensiones en zonas de tableros de distribución y PDUs	X	
Protección contra descargas atmosféricas		X
Sistemas de energía ininterrumpible que soporte el 120 % de la carga existente, más un 30 % para crecimiento	X	
Circuitos derivados de energía ininterrumpible	X	
No más de cinco dispositivos por circuito	X	
Toma corrientes con sistemas de puesta a tierra aislada	X	
Cables de sistema eléctrico identificados en ambos extremos	X	
Resultado (%)	81,82	18,18
Sistema de Aire Acondicionado		
Aire acondicionado de precisión independiente de otras cargas.		X
Resultado (%)	0	100
Instalaciones de Seguridad		
Detección y extinción sencilla de conato de incendio dentro del data center		X
Resultado (%)	0	100
Instalaciones de Comunicaciones	X	
Conexiones entre equipos por medio de Cableado estructurado de par trenzado y/o fibra óptica.	X	
No debe haber conexiones entre gabinetes excepto aquellos que tengan paso directo para cables	X	
Al menos una interfaz de red externa	X	
No debe haber empalmes de ningún tipo de cables de comunicaciones	X	
Los cables deben terminar en ambos extremos con sus conductores o fibras en las posiciones respectivas de los conectores	X	
No deben realizarse conexiones derivadas en serio o paralelo, en ningún punto del trayecto ni en la terminación de cables	X	
Salidas de equipo ubicadas cerca a los equipos activados que conectan	X	
Cableado clase D/categoría 6a, con o sin blindaje, en instalaciones preexistentes		X
Cableado de fibra óptica multimodo OM1 u OM2 sólo en instalaciones preexistentes		X
Longitudes de cableado adecuadas	X	
No debe haber daños ni deformaciones en los cables, cordones, adaptadores o conectores de comunicaciones	X	
Canalizaciones, estructuras, gabinetes, y demás elementos metálicos deben estar conectados al sistema de puesta a tierra de seguridad		X
Penetraciones realizadas en muros y losas para el paso del cableado deben tener sellos que utilicen materiales para barreras contra fuego		X

Los espacios y canalizaciones deben estar protegidos contra: el ingreso de contaminantes, la exposición a agentes que deterioren y condiciones ambientales y mecánicas que puedan afectar la integridad del Cableado Estructurado.	X	
Las instalaciones de Comunicaciones deben tener canalizaciones dedicadas, es decir, no podrán compartirse con otras instalaciones del CPD		X
Las canalizaciones para comunicaciones deben ser metálicas		X
Cualquier tipo de canalizaciones metálica no debe exceder una capacidad máxima del 50% de llenado de cables		X
La capacidad mínima de canalizaciones por gabinete o rack es de 12 cables de par trenzado y 2 cables del 12 fibras ópticas		X
Sistema de administraciones basado en documentación impresa		X
Sistema de administraciones elaborado en computadora	X	
Deben estar identificados todos los enlaces del cableado en ambos extremos, dentro de los primeros 30 cm de su terminación	X	
Todos los racks o gabinetes deben estar identificados en las partes superior e inferior, tanto de la cara frontal como posterior		X
Las etiquetas deben tener durabilidad que garantice la identificaciones del componente durante todo el ciclo de vida del cableado		X
Todas las canalizaciones deben estar identificadas		X
Resultado (%)	52	48
Ámbito u Obra Civil		
Acceso controlado al Data Center		X
Las puertas se deben cerrar automáticamente		X
Abatimiento de la puerta hacia el exterior		X
Barra de pánico instalada en la puerta en caso de emergencia		X
Piso técnico (piso falso o elevado)		X
El piso verdadero o losa no podrá ser menor resistencia a 250 Kg/m^2		X
Iluminación adecuada para ambientes de TIC		X
Mantenerse dentro de los límites de vibración marcados en la Norma		X
Los muros no deberán estar construidos con material de fácil destrucción		X
Ausencia de tuberías hidráulicas y sanitarias dentro del CPD		X
Resultado (%)		100
Sustentabilidad		
Tecnologías tendientes a mejorar la eficiencia energéticas		X
Procesos de virtualización	X	
Aire acondicionado de precisión de capacidad variable		X
Pasillos fríos y calientes		X
Chimeneas en los gabinetes para conducir eficientemente el aire caliente		X

Uso de LED para sistema de iluminación		X
Resultado (%)	16,67	83,33

En la **tabla 2** constan todos los aspectos que cubre la norma para el Nivel I según ICREA 2013, se expresa en porcentaje los aspectos alcanzados según la norma y además, evidencia las deficiencias en el sistema de aire acondicionado (0%), seguridad (0%), obra civil (0%) y sustentabilidad (16,67%). Aunque los sistemas eléctrico (81,82%) y de comunicaciones (52%) están dentro de lo normal, es posible implementar controles para que puedan elevarse al porcentaje que requiere la normativa. La aplicación de la norma ICREA 2013 demuestra que el centro de datos de la institución no se encuentra preparado para afrontar los riesgos tecnológicos inherentes.

4.1.1. Calificación de la probabilidad e impacto del centro de datos del GADMCE

Para la calificación de la probabilidad se ha manejado una escala valorativa del 1 al 4, en relación a la probabilidad de que se materialice el riesgo.

Donde valor de 1 representa la probabilidad baja de producirse la falla del activo debido a que los controles de seguridad son seguros y efectivo; el valor de 2 de probabilidad media de producirse la falla en el activo; valor de 3 indica la probabilidad alta de ocurrencia de falla y valor de 4 que representa a la posibilidad catastrófica, esto evidenciaría que los controles de seguridad son ineficientes. En la **tabla 3** se aprecia la escala valorativa respecta a la probabilidad de falla de controles.

Tabla 3. Escala de probabilidad de falla de activo *(Aguirre & Palacios, 2014)*

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

Para la calificación del impacto, se maneja una escala del 1 al 5 para el impacto en relación al desempeño de los controles de seguridad.

Donde el valor de 1 significa un bajo impacto en los activos de la institución; el valor 2 significa un impacto moderado respecto a una interrupción en las operaciones; el valor 3 es de mediano impacto al momento de falla de operación del activo. En cambio, el valor de 4 es de impacto alto para los activos del centro de datos que son afectados en el aspecto económico, operatividad o prestigio de la institución y el valor de 5 representa al impacto catastrófico al momento de producirse una falla o interrupción de operaciones. A continuación, en la **tabla 4** consta la calificación de impacto de los activos.

Tabla 4. Escala de impacto en activos (Aguirre & Palacios, 2014)

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

Para proceder con la valoración y mapeo de riesgo tecnológico estipulado en el estándar ISO 27002, se debe identificar la infraestructura tecnológica que será objeto de estudio. Se constituye una tabla en donde consta el activo considerado, las observaciones de la auditoria y la relación entre riesgo e impacto. A continuación, la **tabla 5** que corresponde a la matriz de riesgo:

Tabla 5. Matriz de riesgo del centro de datos del GADMCE
Fuente: propia de la investigadora

Tipificación riesgo	Equipamiento y Gestión del centro de datos	Observación en campo	Probabilidad	Impacto	Riesgo
R1	Tablero principal	Esta operativo y buen estado. Ver Anexo 6.	1,0	1,0	1
R2	Tablero By Pass	Esta operativo y buen estado	1,0	1,0	1
R3	Tablero de distribución	Esta operativo y buen estado	1,0	1,0	1
R4	Red eléctrica centro de datos	Esta operativo y buen estado. Ver Anexo 21.	1,0	1,0	1

R5	Generador eléctrico	Esta operativo y buen estado	1,0	1,0	1
R6	Tablero de transferencia automática	Esta operativo y buen estado. Ver Anexo 7.	1,0	1,0	1
R7	UPS	Esta operativo y buen estado. Ver Anexo 11	1,0	1,0	1
R8	Aire acondicionado apropiado para infraestructura tecnológica	No es el requerido para la necesidad. Ver Anexo 8.	3,0	5,0	15
R9	Condensador del aire acondicionado	No pertenece a aire acondicionado de precisión	3,0	5,0	15
R10	Paneles del piso falso	No hay piso falso	3,0	3,0	9
R11	Paneles perforados del piso falso	No hay piso falso	3,0	3,0	9
R12	Ventosa de paneles	No hay ventosa	3,0	3,0	9
R13	Hermetización de pasos de cables	No hay piso falso, por consiguiente no hay paso de cables	3,0	3,0	9
R14	Malla de alta frecuencia	No hay malla de alta frecuencia	4,0	5,0	20
R15	Aterrizaje de pedestales a la malla de alta frecuencia	No hay debido a la ausencia de piso falso, pedestales y malla de alta frecuencia	4,0	5,0	20
R16	Sistema de puesta a tierra	La instalación se realizó bajo los lineamientos establecidos	1,0	1,0	1
R17	Pintura antiestática	Si se usó en la estructura	1,0	3,0	3
R18	Cableado	Se encuentra en mantenimiento constante, tiene por etiquetas cintas donde consta el nombre de la departamento que conecta. Ver Anexo 15.	3,0	3,0	9
R19	Puntos de cobre	En óptimas condiciones	1,0	1,0	1
R20	Racks y accesorios	Se encuentran en excelente estado	1,0	1,0	1
R21	Fibra óptica	Tiene como proveedor a CNT	1,0	1,0	1

R22	Canalización y tuberías	Se encuentran en buen estado	1,0	1,0	1
R23	Sistema de control de acceso	No existe, solo se limita a ingreso de personal autorizado	4,0	5,0	20
R24	Sistema de gestión y monitoreo	Siempre está softwareoperando	1,0	1,0	1
R25	Sistema de detección y extinción de incendios	No existe	4,0	5,0	20
R26	Sistemas de video seguridad	Se encuentra en mantenimiento	4,0	5,0	20
R27	Puerta de seguridad	Existe Puerta básica de acceso. Ver Anexo 19	4,0	5,0	20
R28	Puerta de aluminio	No existe	4,0	5,0	20
R29	Licencia de los servidores	Todos los servidores cuentan con sistemas licenciados	1,0	1,0	1
R30	Respaldo de base de los servidores	Si se realiza respaldo de información, tiempo automatización 1:00 pm- 8:00 pm	1,0	1,0	1
R31	Tecnología de los servidores	Los equipos servidores tienen antigüedad de 5 años	4,0	4,0	16
R32	Servicios tercializados	A razón del administrador si se realizó contratación para servicios del centro de datos, pero no se dio a conocer la documentación adquisiciones	2,0	3,0	6
R33	Capacitación del personal	Se capacita al personal eventualmente	4,0	5,0	20
R34	Administración de recursos	Las funciones se cumplen a cabalidad según responsabilidades del personal	1,0	1,0	1
R35	Informes de monitoreo	El sistema empleado genera reportes constantemente. Ver Anexo 17	1,0	1,0	1

R36	Documentación técnica	El administrador no facilitó la documentación por considerarla reservada, aunque declaró de perdida de documentación referente a la estructura de red	3,0	5,0	15
R37	Políticas	Cada acción se la realiza en coordinación con el Jefe de Sistemas	1,00	1,00	1

4.1.2. Intervalos de riesgos de los activos del centro de datos del GADMCE

En la **tabla 6** se presenta los intervalos de rangos de riesgos de falla o interrupción de las operaciones de los activos pertenecientes al centro de datos.

Tabla 6. Intervalos de riesgos para activos del centro de datos (Aguirre & Palacios, 2014)

Tabla de riesgos	
Riesgo 1>=5	Bajo
Riesgo 6>=10	Medio
Riesgo 11>=15	Alto
Riesgo 16>=20	Catastrófico

4.1.3. Priorización de los activos del centro de datos del GADMCE según riesgos

Es necesario identificar los activos del centro de datos que tengan calificación de riesgos medio, alto o catastrófico, se descarta los riesgos bajos. En la **tabla 7** se muestra los riesgos que pueden materializarse.

Tabla 7. Priorización de riesgos del centro de datos GADMCE
Fuente: propia del investigador

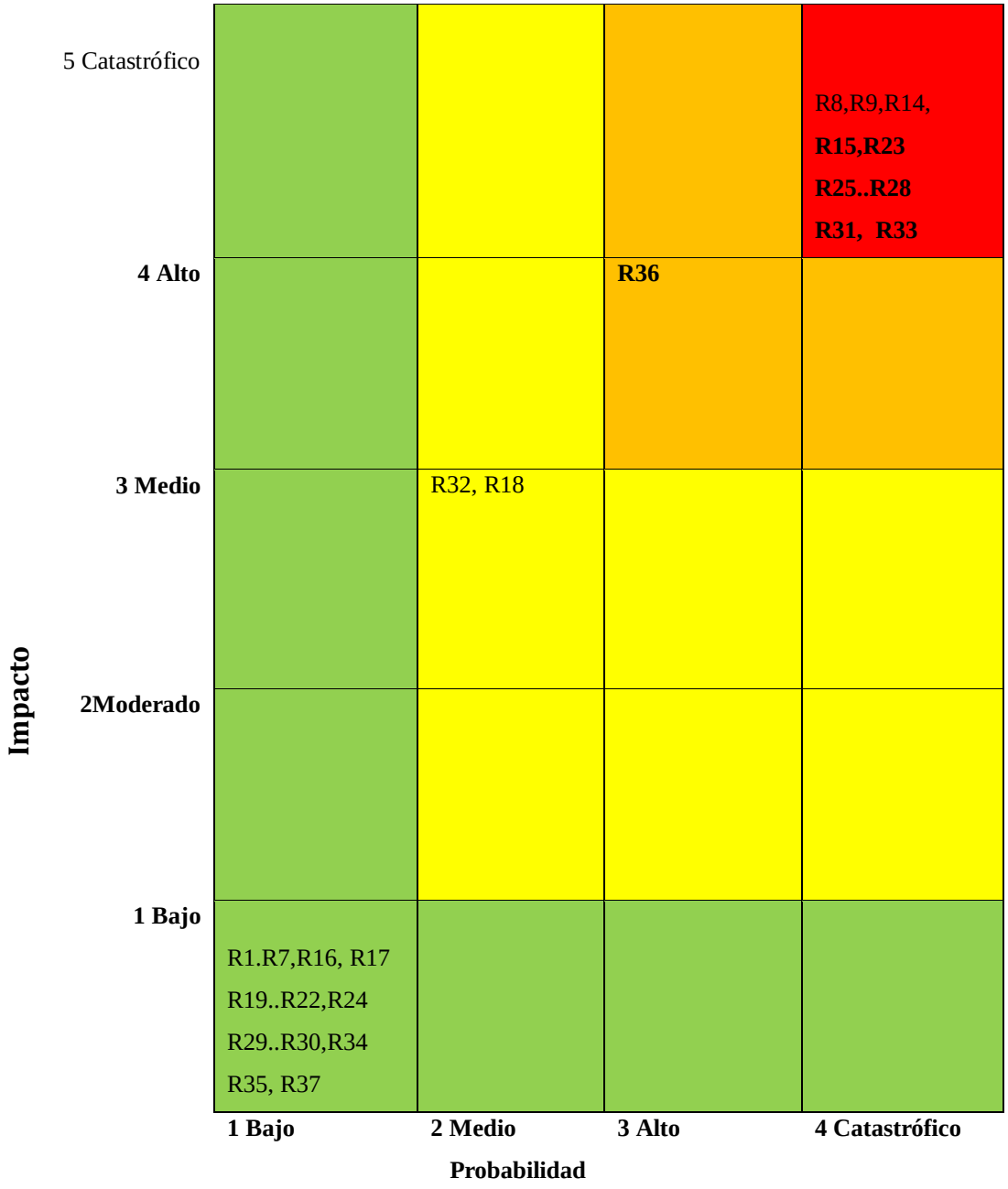
Tipificación riesgo	**Equipamiento y Gestión del centro de datos**	**Probabilidad**	**Impacto**	**Riesgo**
R8	Aire acondicionado apropiado para infraestructura tecnológica	3,0	5,0	15

R9	Condensador del aire acondicionado	3,0	5,0	15
R10	Paneles del piso falso	3,0	3,0	9
R11	Paneles perforados del piso falso	3,0	3,0	9
R12	Ventosa de paneles	3,0	3,0	9
R13	Hermetización de pasos de cables	3,0	3,0	9
R14	Malla de alta frecuencia	4,0	5,0	20
R15	Aterrizaje de pedestales a la malla de alta frecuencia	4,0	5,0	20
R18	Cableado	3,0	3,0	9
R23	Sistema de control de acceso	4,0	5,0	20
R25	Sistema de detección y extinción de incendios	4,0	5,0	20
R26	Sistemas de video seguridad	4,0	5,0	20
R27	Puerta de seguridad	4,0	5,0	20
R28	Puerta de aluminio	4,0	5,0	20
R31	Tecnología de los servidores	4,0	4,0	16
R32	Servicios tercializados	2,0	3,0	6
R33	Capacitación del personal	4,0	5,0	20
R36	Documentación técnica	3,0	5,0	15

Prioridad

La **tabla 8** se conforma por los códigos de los activos del centro de datos en cuadrantes correspondientes según el impacto y probabilidad calculada.

Tabla 8. Prioridad de riesgo
Fuente propia del investigador



4.1.4. Evaluación aplicando controles según Norma ISO/IEC 27002

Para tratar los riesgos es necesario la implementación de controles a los riesgos señalados con mayor probabilidad de materializarse y repercusión. A continuación, en la **tabla 9** se establecen controles.

Tabla 9. Cuadro de controles para riesgos
Fuente propia del investigador

Tipificación riesgo	Equipamiento y Gestión del centro de datos	Probabilidad	Impacto	Riesgo	Control
R8	Aire acondicionado apropiado para infraestructura tecnológica	3,0	5,0	15	Adquisición e instalación de aire acondicionado de precisión
R10	Paneles del piso falso	3,0	3,0	9	Instalación de piso falso incluyendo la hermetización de paso de cables
R11	Paneles perforados del piso falso	3,0	3,0	9	
R12	Ventosa de paneles	3,0	3,0	9	
R13	Hermetización de pasos de cables	3,0	3,0	9	
R14	Malla de alta frecuencia	4,0	5,0	20	Instalación de malla de alta frecuencia
R18	Cableado	3,0	3,0	9	Etiquetar debidamente los cables
R23	Sistema de control de acceso	4,0	5,0	20	Sistema biométrico con bitácora virtual
R25	Sistema de detección y extinción de incendios	4,0	5,0	20	Implementación de sistema contraincendios indicado para preservación de equipos electrónicos
R26	Sistemas de video seguridad	4,0	5,0	20	Sistema de video vigilancia de circuito cerrado
R27	Puerta de seguridad	4,0	5,0	20	Instalación de puerta de seguridad
R31	Tecnología de los servidores	4,0	4,0	16	Adquisición de servidores
R33	Capacitación del personal	4,0	5,0	20	Desarrollar plan de capacitación del personal
R36	Documentación técnica	3,0	5,0	15	Desarrollo de biblioteca de documentación técnica

4.1.5. Informe de Auditoria

4.1.5.1. Objetivo del informe

Verificar el cumplimiento de controles de seguridad que tiene el centro de datos del GADMCE en base a los controles establecidos en la norma ISO/IEC 27002.

4.1.5.2. Alcance del informe

La elaboración del informe comprende la validación de los controles que tiene el centro de datos del GADMCE aplicando la norma ISO/IEC 27002.
El informe se dará a conocer al Jefe de la Unidad de Sistemas para el análisis los hallazgos y las recomendaciones que se le sugiere, para posteriormente, proceder con la toma de decisiones respectiva.

4.1.5.3. Metodología utilizada: auditoria de activos basada en riesgos

Para la elaboración del informe se recopiló información mediante entrevistas al personal relacionado directamente con centro de datos del GADMCE y observación de cada elemento de la infraestructura informática.

4.1.5.4. Hallazgos

4.1.5.4.1. No contar con un aire acondicionado de precisión.

Se cuenta con un aire acondicionado básico que no es el correcto para la función que cumple y conlleva al sobrecalentamiento de los servidores.

4.1.5.4.2. No contar con piso falso

No se garantiza el adecuado alojamiento de las instalaciones eléctricas y el cableado estructurado. El cableado estructural e instalaciones eléctricas están expuestas en el centro de datos y proclives a manipulaciones de personal no calificado.

4.1.5.4.3. No contar con malla de alta frecuencia

No se tiene malla de alta frecuencia que actué contra inconvenientes de tipo electromagnético lo que provoca mal funcionamiento de los equipos electrónicos. La malla de alta frecuencia junto con el sistema de puesta tierra brinda protección a los equipos.

4.1.5.4.4. No tener el cableado estructurado correctamente etiquetado

No se tiene las etiquetas perdurables en los cables de red. El material empleado para etiquetas los cables de la estructura de red no es el correcto. Es susceptible a rasgarse o borrarse las letras.

4.1.5.4.5. No contar con sistema de control de acceso

No se tiene un sistema de control de acceso que cumpla con las funciones de identificación y validación del personal que ingresa al espacio destinado para el centro de datos. No hay bitácora virtual que consten las identificaciones del personal que accede al espacio. Sólo contar con la restricción de ingreso es una regla que fácilmente se puede quebrantar.

4.1.5.4.6. No contar con sistema de detección y extinción de incendio

No se tiene un sistema de detección y extinción de incendios exponiendo la necesidad de protección al activo principal de la institución que es la información. Considerando que no se cuenta con un aire acondicionado que garantice la correcta climatización del espacio, el centro de datos se encuentra vulnerable ante un posible incendio.

4.1.5.4.7. No contar con sistema de video seguridad

No contar con un sistema de video seguridad o de circuito cerrado vulnera la seguridad del centro de datos. Al no grabar los eventos que se suscitan en el interior expone el espacio a robos o daños de terceros considerando que no existe un sistema de control de acceso.

4.1.5.4.8. No contar con Puerta de seguridad

No tener una puerta que garantice la seguridad necesaria, vulnera el activo de la información alojado en el centro de datos. El empleo de una puerta de seguridad que sea robusta garantiza la integridad, no solo del centro de datos, sino también del personal

del departamento; tomando en cuenta que no hay sistema de climatización que evite el sobrecalentamiento de los equipos, da la posibilidad de incendios que fácilmente puede propagarse.

4.1.5.4.9. No tener servidores con garantías vigentes

No tener servidores que tengan garantía dificulta el mantenimiento. Sin garantía de fábrica el soporte técnico ante posibles daños no estaría cubierto. Es necesario proteger el activo de la información alojándola en servidores calificados en su totalidad.

4.1.5.4.10. Capacitación del personal

Durante el proceso de auditoría, el administrador manifestó que el personal recibe capacitación relacionada con el centro de datos eventualmente. No tener un plan de capacitación aprobada que se dé periódicamente, expone al personal a la desactualización de conocimientos que se reflejaría negativamente en el desarrollo de sus funciones.

4.1.5.4.11. Documentación técnica

El administrador no mostró toda la documentación durante la auditoria, declaró que la información es reservada. Presentó el informe de instalación de puntos de red del edificio Conservatorio, diagrama unifilar del sistema eléctrico centro de datos, diagrama de enlaces de red del edificio y una captura de pantalla del sistema de monitoreo, también del sistema de auditoria. Pero, manifestó que el diagrama del cableado estructural del centro de datos se perdió. No se puede perder ningún documento que contenga información del centro de datos. Se dio que se realiza acciones coordinadas por el Jefe de sistemas, más no las políticas en detalle.

4.1.5.5. Recomendaciones

4.1.5.5.1. Se debe realizar la adquisición de un aire acondicionado adecuado para la función, que garantice la temperatura correcta en el centro de datos.

4.1.5.5.2. Se sugiere la instalación del piso falso para garantizar la integridad de los cables e instalaciones eléctricas. Al instalar el piso falso se debe considerar los paneles movibles, los paneles perforados y el paso de cables, estos elementos ayudan a mantener las condiciones de temperatura idóneas.

4.1.5.5.3. Se debe instalar la malla de alta frecuencia debido a la protección equipos electrónicos.

4.1.5.5.4. Se sugiere el empleo de material para etiquetado perdurable, por la razón que deben ser resistentes y el nombre del departamento que conecta debe ser legible.

4.1.5.5.5. Se debe realizar la adquisición de un sistema de control de acceso confiable y que realice el registro de identificación del personal que ingresa al centro de datos.

4.1.5.5.6. Se debe adquirir e instalar un sistema de detección y extinción de incendios que garantice la integridad del activo en caso de darse eventuales perjudiciales.

4.1.5.5.7. Se debe adquirir un sistema de video seguridad que registre en tiempo real cada actividad dentro del centro de datos, además, de presentarse eventualidades como robo o daño intencional proveería de importante evidencia.

4.1.5.5.8. Se debe adquirir e instalar una puerta de seguridad hecha de acero y que sea hermética. Estas características ayudan a mantener la integridad de la información y la protección de activos y del personal que labora en el departamento. En caso de darse un incendio, impide la propagación del fuego hacia el exterior.

4.1.5.5.9. Se debe adquirir equipamiento servidor que cuente con garantías vigentes debido a la importancia de su función, el alojamiento de servicios e información de una institución pública vital para las actividades del cantón. No se puede dar la posibilidad de interrupción de actividades debido a daños no cubiertos por garantía.

4.1.5.5.10. Se debe elaborar un plan de capacitación periódica del personal que labora directamente en el centro de datos. Los profesionales del área de sistemas deben estar altamente calificados debido a la importancia de su actividad, mantener la operatividad de los servicios.

4.1.5.5.11. Se sugiere la elaboración de una biblioteca de documentación técnica con la finalidad de organizar y centralizar informes con respecto a las actividades en el centro de datos. Además, se garantiza no perder documento alguno.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La situación en la que se encuentra el Centro de Datos del GADMCE muestra que no alcanza los requerimientos básicos en seguridad que una infraestructura tecnológica debe lograr.

- Por no tener plan de tratamiento de riesgos formal, el Centro de Datos es susceptible a incidentes que afectaría notablemente al personal que labora en las dependencias. La aplicación de los controles sugeridos garantizarían un la integridad y disponibilidad de la información.

- El análisis de riesgo tecnológico es el proceso de evaluación de los activos del centro de datos para poder determinar el nivel de seguridad y proponer mejoras, de ser necesarias.

- La investigación determina que el personal de la Unidad de Sistemas no se rige a procesos de seguridad con respecto al Centro de Datos.

5.2. Recomendaciones

- Elaborar un plan de tratamiento de riesgo para hacer frente a los riesgos detectados durante la realización del proyecto. Tomarlo como una medida de seguridad que debe realizarse periódicamente.

- Desarrollar un programa de capacitación para el personal, con aprobación de presupuesto para su realización y que sea elaborado en base a las necesidades del Centro de Datos de la institución.

- Es necesario concientizar sobre la importancia de la seguridad de activos de la información, alojados en el Centro de Datos. Es necesario implementar medidas de protección.

- Considerar los resultados del análisis de riesgo tecnológico al que fueron sometidos los activos del Centro de Datos, para elaborar un plan de contingencia para la infraestructura.

REFERENCIAS

6.1. Referencias bibliográficas

(2016). Obtenido de GAD de Esmeraldas: http://www.municipioesmeraldas.gob.ec/

AENOR. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.*

Aguirre, D., & Palacios, J. (Marzo de 2014). *Evaluación técnica de seguridades del data center del municipio de Quito segun normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.*

Alférez, C. &. (2012). *Red Inalámbrica de datos y video vigilancia con CCTV para mejorar el servicio de comunicación y seguridad en las instalaciones del Hotel Wendy's.*

Bello, F. (2013). La Investigación Tecnológica: o cuando la solución es el problema. *FACES*, 14.

Castillo, C. (2013). *Secretaria Nacional de la Administración Pública*. Recuperado el 30 de 12 de 2016, de http://www.administracionpublica.gob.ec/biblioteca/

Castro, A. R., & Bayona, Z. O. (2011). *Gesttón de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.*

CNT Sala de Prensa. (2015). Recuperado el 18 de 02 de 2017, de http://corporativo.cnt.gob.ec/cnt-unica-empresa-publica-en-el-ecuador-que-obtiene-certificacion-iso-27001/

Código Orgánico Integral Penal Suplemento N°180. (10 de Febrero de 2014). Obtenido de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Consultor, G. (10 de 2013). *Controles ISO 27000*. Obtenido de http://iso27000.es/download/ControlesISO27002-2013.pdf

Dirección de Comunicación del Ministerio de Coordinación de la Política y Gobiernos Autónomos Descentralizados. (2011). COOTAD.

Fernandez, A. (2016). *Infosecurityvip*. Obtenido de http://www.infosecurityvip.com/newsletter/papers/ISEC%20INFOSECURITY%20SANTO%20DOMINGO%202016%20-%20CISCO%20-%20TENDENCIAS%202016.pdf

Fine, L. H. (2002). *Seguridad en centros de cómputo.* México, Trillas.

GADMCE. (2017). Esmeraldas, Esmeraldas, Ecuador.

Gómez V., Á. (2011). *Enciclopedia de la Seguridad Informática.* México: Grupo Alfaomega Ra-Ma de C.V.

Guamán Carrión, M. (2015). *Proveer criterios y directrices para diseñar, construir e implementar el Centro de Datos para el GAD de Loja, basada en la norma internacional ICREA-Std-131-2013 con aplicabilidad a normas y regulaciones nacionales.* Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/23067/1/tesis.pdf

Heredia. (2015). *Control interno y su incidencia en el proceso administrativo y financiero de la empresa comercial "Distribuidora Mendoza" de la ciudad de El Empalme año 2014.*

iso27000.es. (2012). *El portal de ISO 27001 en español*. Obtenido de iso27000.es: http://www.iso27000.es/sgsi.html

Miler, M. (2008). *Introducción a la informática* (2008 ed.).

Moreno, ,. L. (2010). Las seguridades informática en el trabajo con la plataforma "moodle". *Revista de humanidades*.

MUNICIPIO-ESMERALDAS. (2016). *ALCALDIA DE ESMERALDAS*. Recuperado el 18 de Noviembre de 2016, de http://www.municipioesmeraldas.gob.ec/lotaip/2015/Organigrama_Institucional_v_f.pdf

Onofre, D. (2015). *Diseño de la Infraestructura Física del Data Center en el Gobierno Autónomo Descentralizado Municipal de San Pedro de Pimampiro Basado en la Norma Internacional ICREA-STD-131-2013.*

Ortiz, H. (22 de Mayo de 2013). *Riesgo Tecnológico Definiciones y Origen*. Obtenido de Riesgo Tecnológico: http://riesgotecnologico.blogspot.com/

Peña, J. (2 de Febrero de 2010). *Metodologías y normas para el análisis de riesgos.* Obtenido de ISACA: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

Ramirez, A., & Ortiz, Z. (2011). Gestión de Riesgos tecnlógicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, Vol. 16*, 56-66. Obtenido de Gestión de Riesgos tecnologicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.

Registro Oficial No. 78. (2009). Recuperado el 30 de 12 de 2016, de http://www.azuay.gob.ec/imagenes/uploads/File/BANCO%20DE%20LEYES/12.-

%20NORMAS%20DE%20CONTROL%20INTERNO%20DE%20LA%20CONTRALORIA%20GENERAL%20DEL%20ESTADO.pdf

Rodríguez, G., Gil, J., & Garcia, E. (1996). *Investigación Calitativa.* España: Ediciones Aljibe.

Toddle. (s.f.). Recuperado el 17 de 02 de 2017, de http://toddleoutsourcing.es/tecnologia/seguridad/implementacion-sgsi/

Valdez, H. (08 de 2013). *Sala de prensa: Valdez Albizu informa Banco Central obtiene certificación ISO 27001*. Recuperado el 27 de 02 de 2017, de Banco Central de la República Dominicana: http://www.bancentral.gov.do/notas_bc/2012/05/30/56/valdez-albizu-informa-banco-central-obtiene-certificacion-iso-27001-

6.2. Anexos

Anexo 1

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Guía de entrevista Para el Jefe de la Unidad de Sistemas

Trabajo de Grado: "Análisis de Riesgo Tecnológico del Centro de Datos basado en normas internacionales: caso GADMCE"

Objetivo: Investigar los aspectos administrativos respecto al centro de datos del GADMCE.

1. **¿Cómo se encuentra estructurado la unidad de sistemas?**

2. **¿Cuáles los procedimientos administrativos a realizar en la unidad respecto al centro de datos?**

3. **¿En la unidad de sistemas, cuentan con plan estratégico de Tecnologías de la Información?**
4. **¿Se cuenta con plan operativo?**

Anexo 2

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Guía de entrevista Para el Administrador del Centro de Datos

Trabajo de Grado: "Análisis de Riesgo Tecnológico del Centro de Datos basado en normas internacionales: caso GADMCE"

Objetivo: Identificar las vulnerabilidades de los equipos alojados en el centro de datos del GADMCE.

1. **¿El centro de datos tiene un ambiente físico apropiado para su buen funcionamiento?**

2. **¿Cuenta con registro de ingreso al centro de datos?**

3. **¿Cuenta con estándares de en el centro de datos del GADMCE?**

4. **¿Cuenta con plan de tratamiento de riesgo para el centro de datos del GADMCE?**

Anexo 3

Pontificia Universidad Católica del Ecuador | SEDE ESMERALDAS

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Guía de entrevista Para el Jefe de Mantenimiento Técnico

Trabajo de Grado: "Análisis de Riesgo Tecnológico del Centro de Datos basado en normas internacionales: caso GADMCE"

Objetivo: Identificar las vulnerabilidades de los equipos alojados en el centro de datos del GADMCE.

1. **Indique los sistemas con los que cuenta el centro de datos del GADMCE.**

2. **¿los equipos a su cargo que se encuentran en el centro de datos han tenido inconvenientes en el funcionamiento?**

3. **En caso de responder afirmativamente, ¿explicar cuál fue la eventualidad?**

4. **¿ha sido necesaria la contratación de terceros para actividades relacionadas con el centro de datos?**

Anexo 4

Pontificia Universidad Católica del Ecuador | SEDE ESMERALDAS

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Guía de entrevista Para el Jefe Desarrollo de Software

Trabajo de Grado: "Análisis de Riesgo Tecnológico del Centro de Datos basado en normas internacionales: caso GADMCE"

Objetivo: Identificar las vulnerabilidades de los equipos alojados en el centro de datos del GADMCE.

1. **Indique los sistemas con los que cuenta el centro de datos del GADMCE.**

2. **¿los equipos a su cargo que se encuentran en el centro de datos han tenido inconvenientes en el funcionamiento?**

3. **En caso de responder afirmativamente, ¿explicar cuál fue la eventualidad?**

4. **¿ha sido necesaria la contratación de terceros para actividades relacionadas con el centro de datos?**

5.2.2 Fotografías de la auditoria

Anexo 5

Figura 6. Servidores. Autoría propia.

Anexo 6

Figura 7. Tablero principal. Autoría propia

Anexo 7

Figura 8. Tablero de transferencia. Autoría propia.

Anexo 8

Figura 9. Aire acondicionado básico. Autoría propia

Anexo 9

Figura 10. Servidores toma de lejos Autoría propia

Anexo 10

Figura 11. Racks y UPS. Autoría propia

Anexo 11

Figura 12. UPS. Autoría propia

Anexo 12

Figura 13. Equipo Cisco. Autoría propia.

Anexo 14

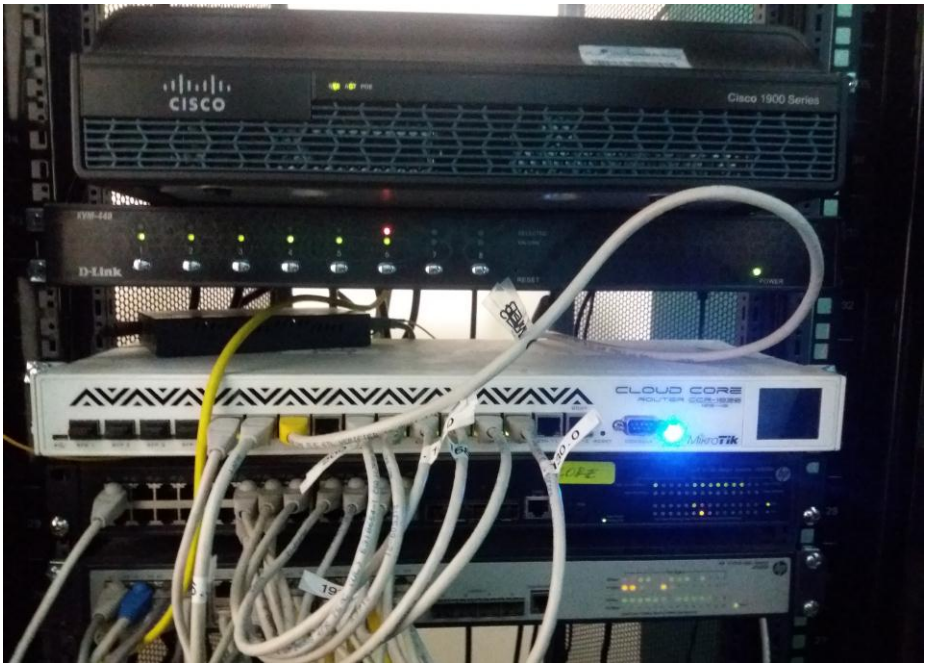


Figura 15. Equipo Cisco y Cloud MikroTik. Autoría propia.

Anexo 15

Figura 16. Etiquetas en el cableado. Autoría propia.

Anexo 17

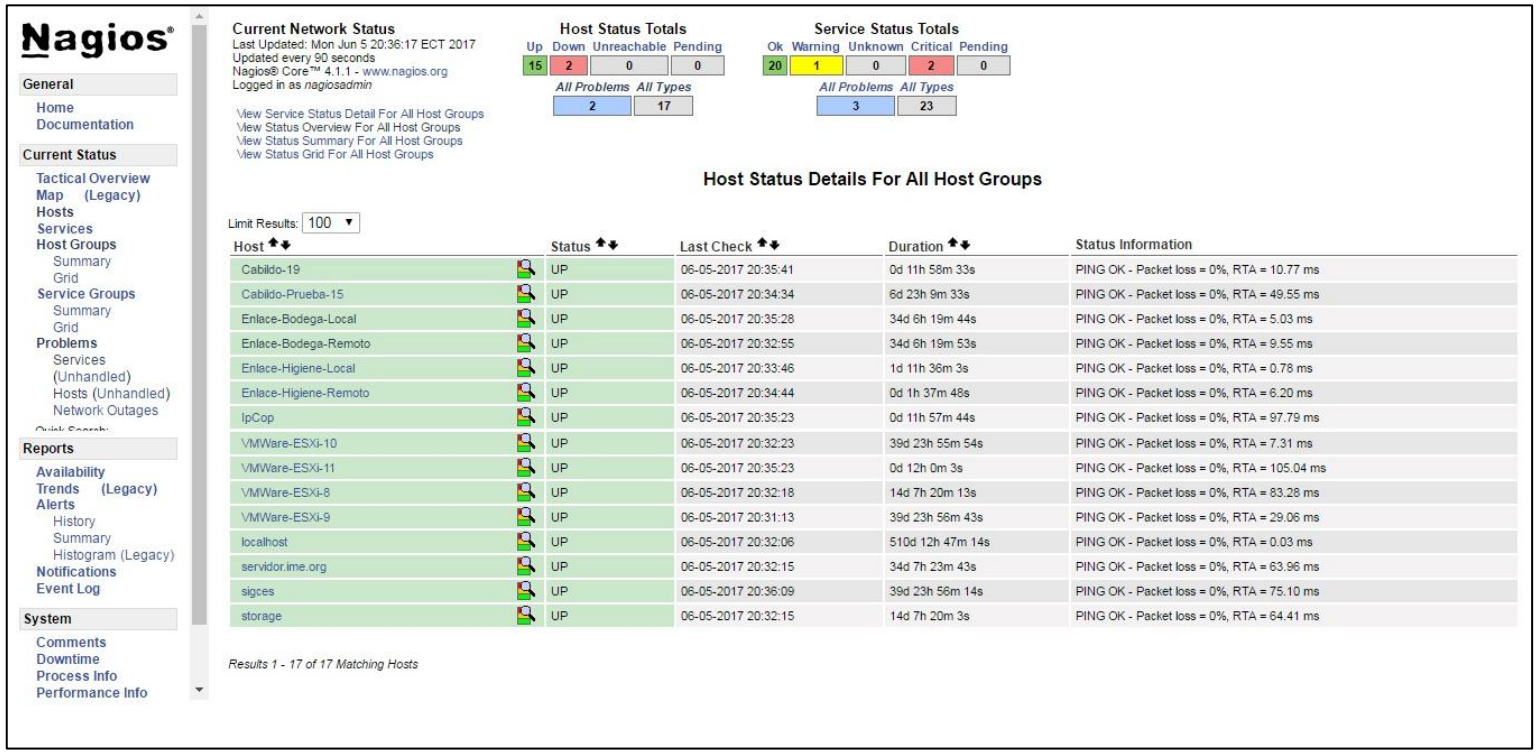


Figura 18. Captura de pantalla del sistema de monitoreo de aplicativos. Autoría propia

Anexo 18

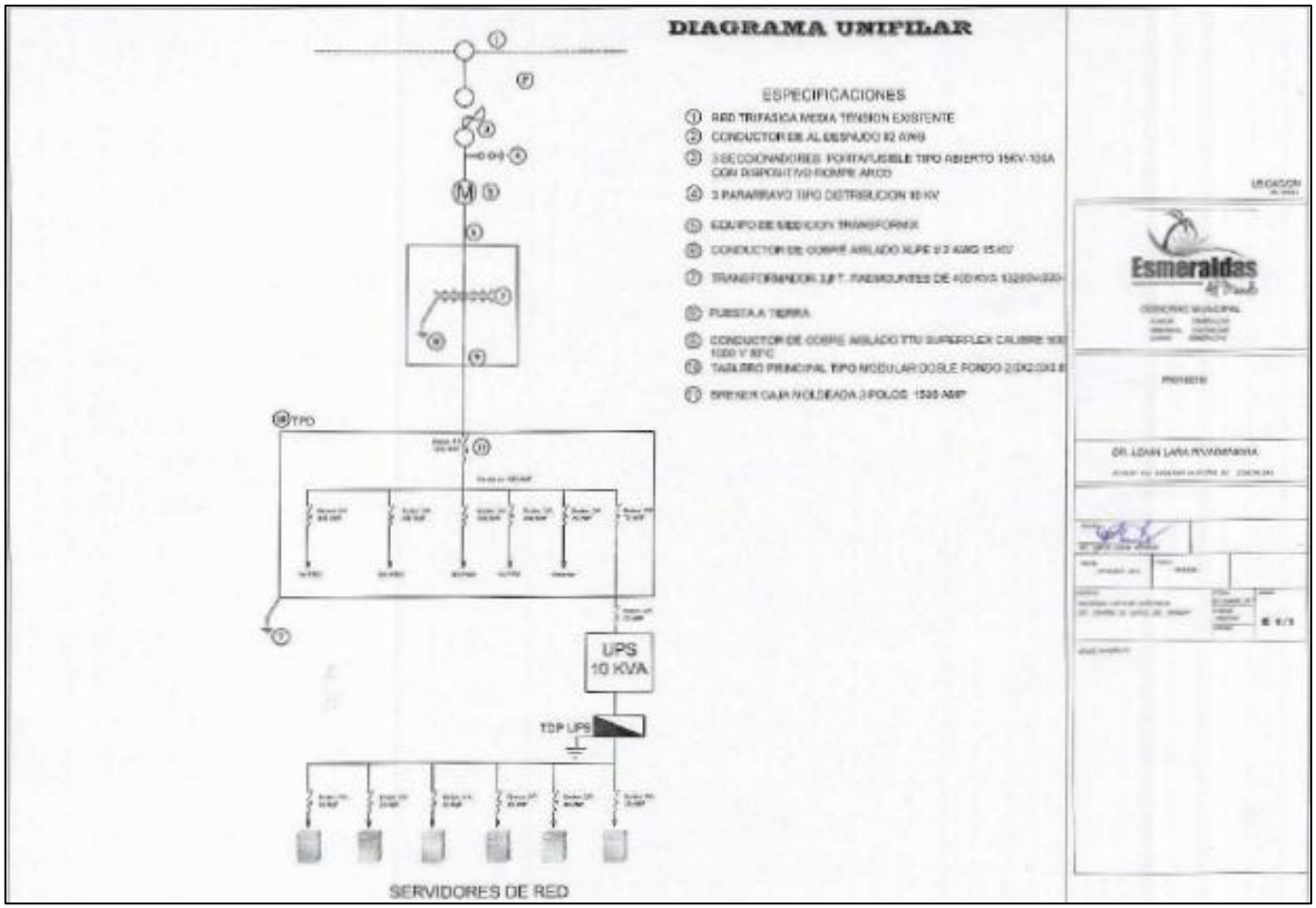


Figura 19. Diagrama Unifilar de red eléctrica Autoría Especialista eléctrico. Autoría propia

Anexo 19

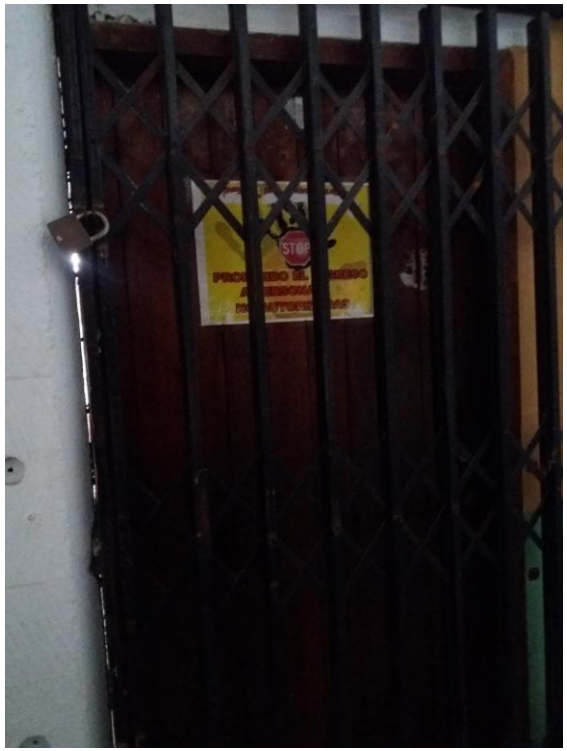


Figura 20. Puerta para acceso a Centro de Datos. Autoría propia

Anexo 20

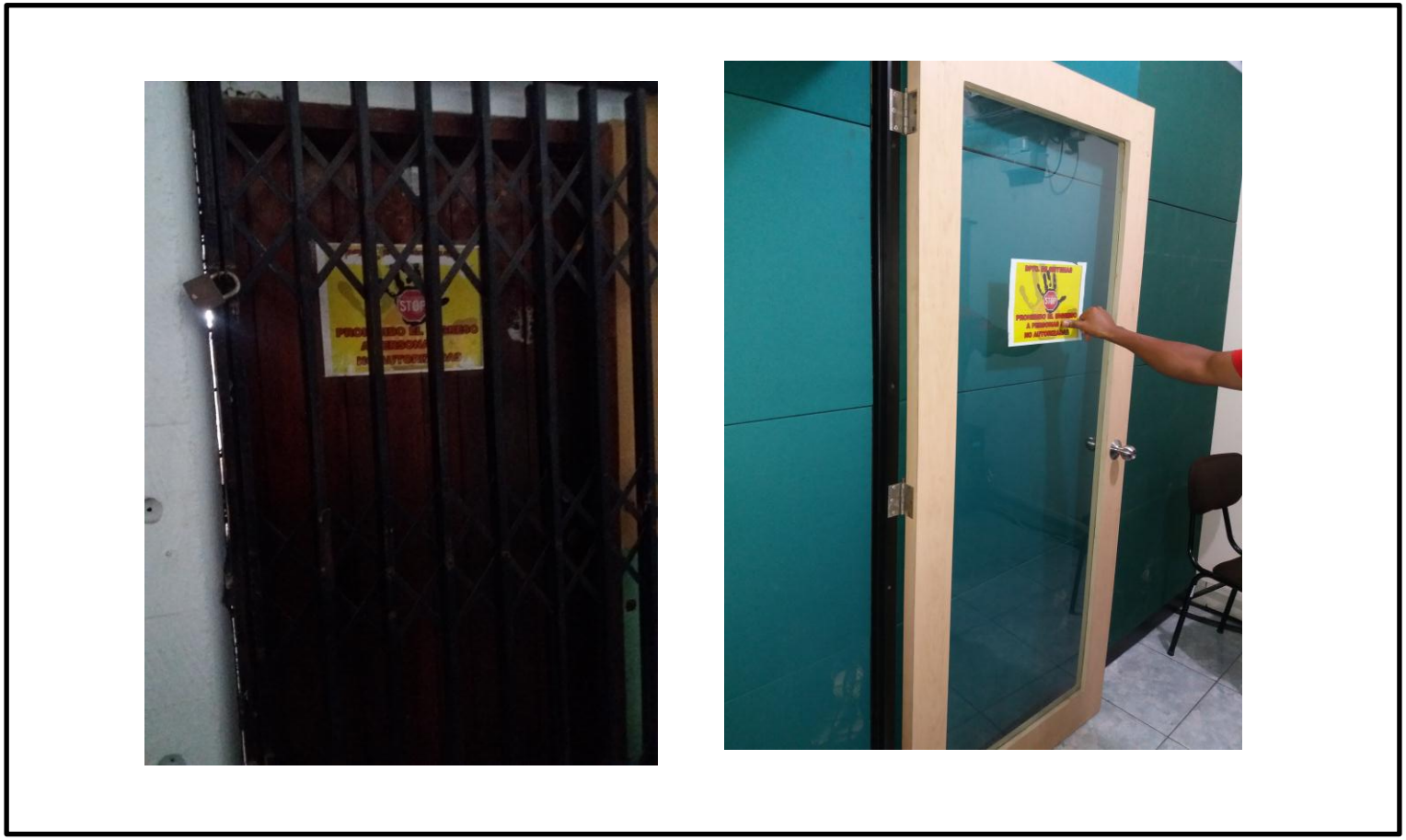


Figura 21. Puerta para acceso a Centro de Datos. Autoría propia

Anexo 21

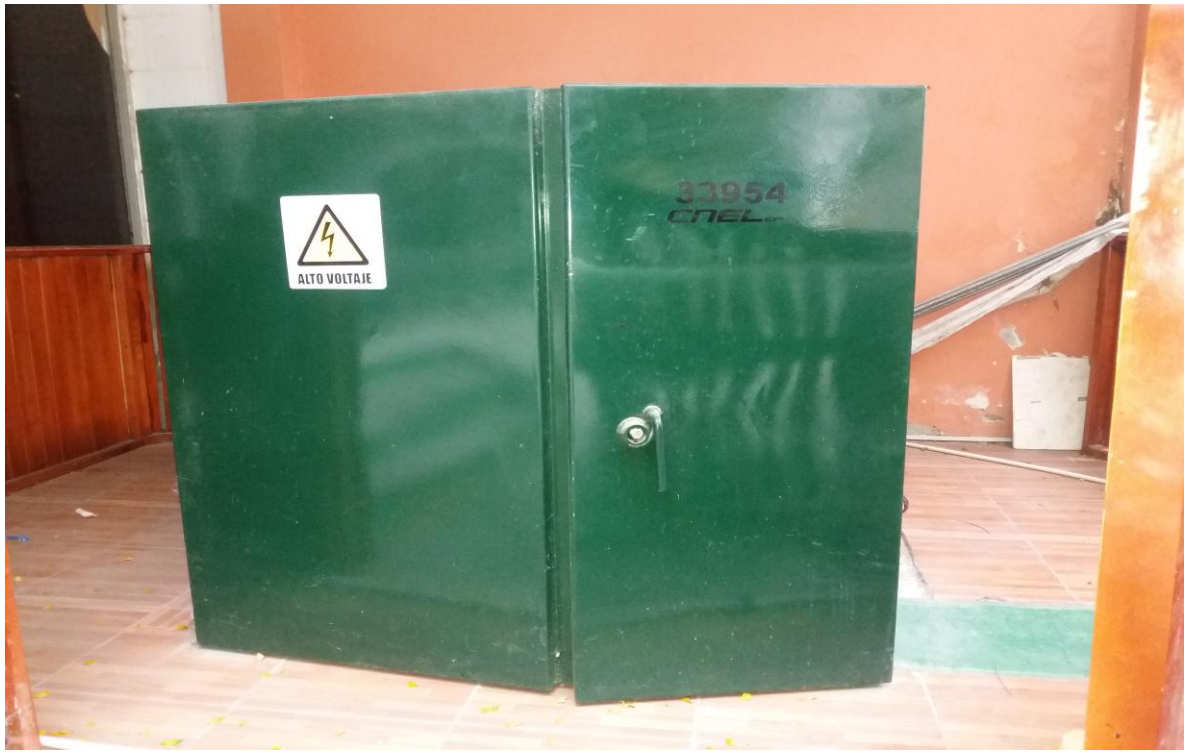


Figura 22. Puerta para acceso a Centro de Datos. Autoría propia